CHILDREN'S TEXT PASSWORD BEHAVIORS AND PARENTAL ADVICE

by
Sumbal Maqsood

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF COMPUTER SCIENCE

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
April, 2018

Abstract

With increasing use of technology and the Internet among children, it is imperative to understand how they create passwords to protect their personal information, and also the parental advice they get to create these passwords. To understand this, we conducted two studies. The first study was conducted with children ages 11 to 13 to understand their password practices. The second study was conducted with parents to understand their own password behaviors and the strategies they teach their children to create secure passwords. The results of the studies indicated that children between ages 11 to 13 create simple passwords but believe that these passwords are hard for a stranger to guess. We also found that parents are concerned about their child's safety, but parents who are more aware of security-related cues are more likely to create secure passwords and teach their children to do the same.

Acknowledgements

I would like to thank my supervisors, Prof. Robert Biddle and Prof. Sonia Chiasson for the patience, guidance, encouragement, and advice provided throughout my thesis. Their guidance, flexibility, and support helped me complete my thesis while working full-time.

I would also like to thank my thesis committee members for reading my thesis and conducting the defense: Prof. Anil Somayaji, Prof. Kasia Muldner, and Prof. Christopher Joslin

Lastly, I would like to thank my sister, Sana, for providing support and especially in helping me prepare for the defense. I would also like to thank my mom for continuous encouragement, love, and moral support, without which it would have been difficult to complete my thesis.

Table of Contents

Abstract ii

Acknowledgements iii

Chapter 1 Introduction 1

Chapter 2 Related research 4

2.1 Children's understanding of safety and security 5

2.2 Text-based authentication for children 8

2.3 Graphical based authentication for children 10

2.4 Alternative methods of authentication for children 14

Chapter 3 Study 1 : Lab study of alphanumeric password rules 16

3.1 Study Design 16

3.1.1 Participants 16

3.1.2 Methodology 16

3.2 Results 21

3.2.1 Creation time 21

3.2.2 Login time 23

3.2.3 Recall 26

3.2.4 Passwords 27

3.3 Discussion 33

Chapter 4 Study 2: Evaluating parents' awareness of security and their children's password behaviors 39

4.1 Study design 39

4.2 Survey structure 39

4.3 Method 40

4.4 Participant recruitment 41

4.5 Participant demographics 41

4.6 Results 42

4.6.1 Parents' awareness of security cues and their password creation practices . . . 42
4.6.2 Parents' concerns about their child's password practices and the threats to which the child is exposed . . . 47
4.6.3 Parents' beliefs and practices about creating passwords and practicing safe online behaviors . . . 50
4.6.4 Composite variables . . . 56
4.7 Discussion . . . 62
4.7.1 Parent participants' level of concern and teaching their child to create secure passwords . . . 63
4.7.2 Parent participants' level of awareness and teaching their child to create secure passwords . . . 64
4.7.3 Conclusion . . . 65

Chapter 5 Conclusions **67**
5.1 Study 1: Findings . . . 67
5.2 Study 2: Findings . . . 68
5.3 Limitations . . . 69
5.4 Contributions . . . 69
5.5 Future work . . . 70

Bibliography **72**

Appendix A Study 1: Parental Permission for Children Participation in Research **76**

Appendix B Study 1: Verbal informed assent script for children **79**

Appendix C Study 1: Pre-test questionnaire **80**

Appendix D Study 1: Questionnaire during the study **81**

Appendix E Study 1: Post-test questionnaire **82**

Appendix F Study 1: Password strength using the new strength measure 84

Appendix G Study 2: Informed Consent (Qualtrics) 89

Appendix H Study 2: Recruitment poster (Qualtrics) 91

Appendix I Study 2: Survey - Evaluating parents' awareness of security and their children's password behaviors 92

Appendix J Study 2: List of participants' responses to question "What is the biggest risk to your child's accounts?" 112

Appendix K Study 2: Survey questions considered for the five composite variables 114

Chapter 1

Introduction

Children's access to the Internet has steadily increased over the years. Globally, one-third of Internet users are children [6]. Children younger than 15 years old are online as often as adults [21]. They are primarily connected to the Internet at home using their mobile devices [6]. 99% of Canadian school children are highly connected from outside of school [32]. This increase in connectedness has parents worried about children's safety.

Parents' attitudes towards children's access to the Internet has changed over the years. They used to consider access to the Internet as an opportunity for children to gain information and knowledge. In contrast, parents nowadays no longer consider the Internet as a benefit, rather, it is a source of fear and anxiety [32]. Overall, parents understand that being connected provides children with opportunities to learn, gain knowledge, socialize, engage in issues that matter to them, develop interpersonal skills and practice critical thinking. But it also exposes them to dangers such as cyberbullying, stranger danger, scams and inappropriate content [32]. This is especially true for younger children, who are not as digital-savvy or knowledgeable. Due to these threats, parents extensively monitor their children's activities, even at the expense of breaching their privacy and trust [32]. Children are a vulnerable population, and they need to be protected against these threats.

Children have accounts on various websites and applications such as gaming, email systems or social media websites. Younger children mostly play games or watch funny videos when they are online [32] while older children (11 to 17 year olds) use social networking to engage with their peers/friends, keep up with current events, learn something new or gain information [32]. For these activities, children have accounts on websites or applications which require a username and password. These accounts sometimes contain children's or parents' personal information that needs to

be protected. Parents typically monitor their children's activities and have access to their passwords to ensure that they are safe. However, parents are unable to monitor their children's activities when they are at school, with another family member, or with friends. Children need to be taught at a very early age about online threats and how to better protect themselves against these threats.

There is very little research on how children authenticate and protect themselves online. Research has shown that children have difficulty managing their passwords. They often forget their passwords and engage in poor password management strategies [3, 18, 26]. Parents are also concerned about their children's safety and want to help them manage their passwords [3, 17]. In the thesis, we address the following research questions:

- How do children create passwords given different password rules?
- What strategies parents are teaching their children about creating secure passwords and understanding parents' password behaviors?

To answer these questions, we conducted two studies, the first one to understand children's password practices and the second study to understand parents' password behaviors and the strategies they teach children to create secure passwords. The result of the first study indicated that children between ages 11 to 13 created simple passwords, but think that these passwords are hard for a stranger to guess. This raised the question: are parents teaching children to create weak passwords? The result of the second study indicated that most parents are concerned about their child's safety, but parents who are more aware of security-related cues are more likely to create secure passwords and teach children to do the same.

The outline of this thesis is:

- Chapter 2 outlines the literature in the field of children and security
- Chapter 3 outlines the research conducted to understand children's password behaviors
- Chapter 4 outlines the research conducted to understand parents' password behaviors and what they teach their children about creating secure passwords

- Chapter 5 outlines key findings of our research, design recommendations for authentication systems designed for children and guidelines for parents on teaching children to create secure passwords

Chapter 2

Related research

Authentication, in computer security, is known as identifying oneself to acquire access to information or resources. Passwords remain one of the most commonly used methods of user authentication [4]. Historically, users were referred to as the "weakest link" in the security chain [29]. However, we now understand that users engage in poor security practices because the systems are not designed to meet their needs [2, 35]. Systems designed with a focus only on security and not usability will suffer from users engaging in poor security practices such as, reusing passwords across multiple systems and selecting weak passwords that are easy for them to remember [30, 39]. Thus making users vulnerable to a variety of attacks ranging from shoulder surfing, brute force, and dictionary attacks.

Research has shown that passwords suffer from usability and security problems. Secure passwords are complex and harder for users to remember. Due to this, users often engage in poor coping strategies such as creating weak passwords [30]. Simple passwords are easier for users to remember, but they are vulnerable to attacks. Due to these problems, Bonneau et at al. [4] looked at different authentication schemes to replace passwords. They analyzed various authentication schemes including text-based passwords based on usability, deployability, and security. They found that authentication schemes other than passwords do not offer more benefits than passwords. For example, these other authentication schemes were better in one aspect (security) but worse in another (usability or deployability). The benefits of other authentication schemes did not outweigh the cost of changing existing systems that use passwords or changing users' mental model of authentication. For now, passwords remain as a primary means of authentication.

The primary focus of our research is on authentication systems designed for children. There is sparse literature in this area, but we will go through it in the sections

below to understand the research that has been done so far with children and authentication. The first part outlines children's behaviors and attitudes towards security, their security knowledge and how they choose to protect their personal information. The second and third parts discuss research done with children using text-based passwords and graphical passwords.

2.1 Children's understanding of safety and security

Users often have difficulty creating passwords that are secure and memorable [39]. This problem is even worse when the users are children. Children process information differently than adults. Their knowledge base of information is limited compared to adults, and they are actively learning strategies to remember and recall information [7]. Understanding these limitations and children's behaviors and attitudes towards security will help us design authentication systems that meet their needs.

Read at al. [25] conducted a study with children to understand how they keep their personal information safe and secure. Researchers were concerned that children might change their behavior if they were asked directly. Therefore, they used a "participatory analogy" method, to gather information on how children keep their personal information secure and safe. In the "participatory analogy" method researchers asked questions in an abstract manner that would lead them to understand how children keep their personal information safe. In the study, children completed an activity in which they were asked to draw five important items they would take with them if they and their parents were moving to the moon tomorrow. Then, from the five items, children were asked to pick one special item and tell the researcher how they would keep it safe. Children choose special items that were either experiential (game consoles) or emotional (parents/siblings) for them. To keep emotional items safe, children selected to keep them close (in their bedroom or under their pillow) and to keep experiential items safe they chose to keep them in locked boxes or cupboards in their home. Passwords are like an experiential item; they are used unlock an experience that the child would like to acquire (playing a game or interacting with friends on social media). Therefore, children could be taught to keep their passwords safe by having them write it down and keep it in a safe place such a locked cupboard

or their bedrooms. This approach will help children understand that passwords are information that needs to be kept safe and secure like a special item. The study suggested recommendations for designing instructional material for young children to help them learn to keep their personal information safe.

Rode et al. [28] conducted an exploratory study with children and parents. They found that parents were concerned about their children's safety. However, children did not seem concerned about their safety and expressed behaviors that could put them at risk of potential threats (stranger danger and identify theft). Parents had different types of rules for children to keep them safe. These rules included: limiting the use of computers; installing anti-virus; not opening unknown emails; blocking activities that were deemed as risky (not accepting friend requests from people who children do not know) or threatening (not using some websites or not purchasing online without parents' permission). Parents used different strategies to apply the rules, such as monitoring children's activities through technology; not allowing children to use certain websites; using computers in a shared space; being actively present when children are using the computer. Parents try to protect their children by putting in place rules and monitoring their activities. However, children are not always under the supervision of their parents (school, friends or grandparents' place) and may not follow these rules, putting them at risk of threats.

In another study, Zhang-Kennedy at al. [40] tried to find children's understanding of privacy and perceived threats and parents' perceived threats and protection strategies. They found that most children have a poor understanding of privacy. Their understanding of online privacy is 'to be alone', 'to hide secrets or special things', 'to not talk to strangers'. Only a few children, mostly older, had a basic understanding of online privacy. Similar to Rode et al. [28] they found parents were concerned about children's safety and they used various strategies (monitoring, restricting access to apps, screening list of contacts, checking privacy settings of apps and deleting apps) to protect children against what they deemed as threats (media, technology, and strangers). However, the researchers found a mismatch between children's and parents' understanding of potential threats [40]. Children considered their siblings and friends as a major threat whereas parents considered strangers and media as

major threats. Children believed that their siblings or friends would 'mess-up' their games or send them inappropriate content, which could get them in trouble with their parents. Surprisingly, children did not see strangers as a threat. It seems like children do not know what constitutes a stranger; they thought that people approved by their parents are safe. Parents worried that younger children would have trouble identifying someone as a stranger online if they were nice to the child. Parents tend to employ strategies against external threats more than internal threats, but in reality a breach of a child's security and privacy mostly comes from a trusted adult. Based on the findings, it is obvious that children need to be taught about privacy and security. Researchers recommend developing training material tailored toward children's understanding of privacy and threats, making it easier for them to learn these concepts [25, 40].

Zhang-Kennedy at al. [40] also found that children's accounts are managed by their parents who use poor coping strategies to remember all the different passwords (sharing the password with children or writing it down and not keeping in a safe place). Parents also encourage their children to create weak passwords which can be cracked quickly by a dictionary guessing attack. This is a problem: children at a very young age are being taught to create weak passwords. Children will most likely carry-on these poor password practices into adulthood. Hundlani et al. [17] proposed a new method of authentication to alleviate pressure from parents of having to manage their children's passwords. They developed an application called "Kindersurf" that allows parents to control children's access to different websites. Parents only have to remember one password instead of multiple passwords. Children try to access a website by entering their OpenID username, and parents get a notification to approve or reject children's access to the website. "Kindersurf" makes it easier for children to login since they do not have to create and remember passwords for multiple websites. It also helps improve children's security as parents have to manage one OpenID password and children do not need a password to login. Therefore, it reduces the likelihood of parents writing down the password and children having to create simple and weak passwords. Parents like to monitor their children's activities [28, 40] to protect them against perceived threats. Therefore, parents in Hundlani et al. [17]

study appreciated "Kindersurf" and mentioned that they would use it to manage their children's access to various websites. Children, however, did not feel the same way: they did not like the extra verification step before they can access the website. There are several limitations to this new method: older children can learn to bypass the authentication, and children are not learning to create secure passwords at a young age.

The findings [25, 28, 40] indicate that children do not have good mental models of privacy and how to protect their personal information. They do not understand the implications of their threatening security behavior, therefore, putting them at risk of threats. Further research needs to be conducted to understand why children are not concerned about their safety. It may be that children think that their accounts are not worth protecting (nothing personal), they do not understand that their behaviors are putting them at risks, or they are not fully aware of the kinds of threats that they that they are exposing themselves to. To protect children from perceived threats, parents use strategies such as enforcing rules and monitoring their activities [28, 40] but these strategies do not always work. There is very little research conducted on strategies parents use to teach their children to create secure passwords to protect themselves online. We conducted a study (Chapter 4) to understand the techniques parents teach their children to create secure passwords and protect themselves online.

2.2 Text-based authentication for children

As mentioned in beginning of this section, text-based passwords are commonly used for authentication [1, 4, 16] despite their usability and security problems [14]. Children are constantly exposed to systems that use text-based authentication. Parents use text-based passwords to login to applications that children use, such as YouTube, iTunes, and gaming websites [40]. Schools use applications (Google Classroom/Gmail) that require children to remember text-based passwords. Since text-based passwords are highly prevalent, it is imperative to understand how children create passwords using this authentication system.

Read at al. [25, 26] conducted two studies to understand how children create text-based passwords. The first study was conducted to find out children's understanding

of passwords and what they think makes a 'good' password. The results showed that children's understanding of passwords was different than adults. For children, passwords were used to prevent others from getting access to their information, as opposed to allowing children access to their information. Children considered a simple, easy to remember and hard for others to guess (security) as a 'good' password; thus indicating that they have a basic understanding of a secure password. The second study was used to understand how children would create text-based passwords and usernames with no constraints. The findings were somewhat similar to what children reported in the first study. Children created simple passwords, consisting of whole words rather than random characters. Most of the passwords were not guessable from children's usernames, indicating that children created passwords differently than usernames. Even though passwords were simple, they were not memorable, 50% of the children had difficulty recalling the passwords after 75 minutes. The findings from the studies indicate that children have a basic understanding that passwords are used to protect their information. They have difficulty recalling text-based passwords. The researchers did not look at the detail composition of children's passwords.

In another study, Lamichhane at al. [18] looked at the composition of text-based passwords created by children. The researchers employed a game-based design in their study to make it easier for children to provide information. Gamification allows researchers to collect data from children in fun ways [20] without asking them questions through questionnaires. In the study, children interacted with a character "Rewdon" in an Android application. "Rewdon" animatedly asked the children for information such as their name and age, the name of their best friends and pet, their favorite color, food, cartoon, superhero, sports team and sports hero . At the end of the questions, children created a username and a password, which they used later to login to the application to interact with "Rewdon". Researchers were interested in the composition of children's passwords and memorability. They tested children's usernames and passwords for simplicity and guessability. Passwords were composed of one or two words, 1-5 digits and personal information were either considered simple or moderately simple. Passwords composed of unrelated characters, long set of numbers, mixed character case were considered complex. Passwords that were simple

and included a child's personal information were deemed easy to guess, and passwords that contained two joined words and no obvious easy words were considered hard to guess. The results aligned with researchers' previous work [26]. Children created simple usernames and passwords. 76% of children created usernames composed of self-related information, and 53% of children created passwords with self-related information. Usernames and passwords contained words that were easy to guess. Children also had trouble recalling complex passwords compared to simple and moderately simple passwords. For complex passwords, it took children more than two login attempts to recall their passwords, whereas for simple passwords children recalled them on the first attempt. Similar to findings of Read at al. [26], long and complex text-based passwords were harder for children to remember and recall.

Based on their findings [18, 26], the researchers proposed three design recommendation for text-based authentication systems designed for children. First, systems designed for children should require shorter passwords than adults. Second, the rules for password complexity need be relaxed for systems designed for children. Third, children should be warned about their poor password choices (spelling mistakes, repeated characters, password similar to usernames and sequence of numbers used in the password) during the password creation process to help them learn to create secure passwords. The first and second recommendations might have an impact on security, as short and simple password tend to be easy to guess and crack. There needs to be a balance between usability and security, especially for children. Lamichhane at al. [18] also recommend that other types of authentication such as graphical passwords might be more suitable for children and we will look at these in the next section.

2.3 Graphical based authentication for children

Children have difficulty recalling text-based passwords [18,26]. Text-based passwords are based on free recall. This makes it harder for users to recall long and complex passwords and it is even harder for children. Text-based passwords may not be an ideal method of authentication for children as they make typos and spelling mistakes during password entry [18]. Graphical based authentication might be a better alternative for children.

Graphical passwords are developed with images rather than text. They leverage the picture superiority effect. The picture superiority effect is a psychological phenomenon that suggests people are better at remembering images rather than words [10, 24]. Graphical passwords can be designed to utilize different type of memory retrieval (free-recall, cue-recall or recognition). Research has shown that users are better at retrieving information from memory using recognition than recall [33,36,38].

Cole et al. [9] conducted an exploratory study to understand differences between textual and graphical passwords for children. For their study, the researchers choose PassPoints [37] as the graphical password system. To create a password using PassPoints, users select an image and then pick five points on the image. To login, users choose the same image and pick five points on the image in the same order as they did during password creation. For textual passwords, users created an alphanumeric username and password using the keyboard which they later used to login to the system.

In the study, children created graphical and textual passwords on five different websites. They logged in to each of the sites three times, once right after creating the password, the second time after completing the distraction task (playing a game after creating the password) and the third time after 11 to 16 days from the initial login. The researchers found that the graphical passwords were more memorable than textual passwords for short-term but not the long-term. The success rate of graphical passwords dropped from 87% to 78% after the distraction task and to 42% after two weeks. The success rate for textual passwords dropped from 100% to 81% after the distraction task and to 66% after two weeks. For graphical passwords, children remembered the image they selected and generally where the points were located on the image. They had difficulty in accurately choosing the points on the image. For text passwords, children had similar issues identified by Read at al. [26] and Lamichhane at al. [18]. They had trouble recalling the exact spelling, capitalization, and symbols in their passwords. Cole et al. [9] mentioned that both textual passwords and graphical passwords have limitations. It may be that PassPoints is not an ideal graphical password system for children. It requires accurately recalling the position of the points, which is especially harder for young children. However, these limitations

could be used to develop a different type of graphical password system for children. One such authentication system was proposed by Mendori et al. [22].

Mendori et al. [22] proposed a new graphical password system for primary school children. This new system involved a graphical interface with icons, status indicator and various buttons (clear, login, reset, determination). To create a password, children had to select some icons on the interface and click the "determination" button. The "determination" button was used to indicate that the user was done inputting their password. During login, children are presented with the same graphical interface as earlier. To login, they had to select same icons as they did during password creation. The order of icons is randomized during every login to prevent the password to be guessed through shoulder surfing. The researchers put in a lot of effort into identifying icons that would be most suitable for young children and the correct number of icons that should be presented on the interface. A few icons would provide children with fewer combinations and might make it easier for someone to guess the password. Too many icons might confuse children and cause them to make selection errors.

The researchers initially started with 125 icons and through children's feedback narrowed the selection down to 65 icons. To determine the ideal number of icons to be presented on the interface, researchers created three password interfaces with the varying number of icons. The first interface contained eight icons; the second included 16 icons and the third contained 64 icons. A study was conducted with primary school children to find out which of the three interfaces would create the least amount of selection errors and take the least amount of time to enter the password. The result showed that the children made zero selection errors in the first interface; this was expected since it only had 8 icons. Children made fewer selection errors and took the least amount of time to login using the second interface (16 icons). Mendori et al. [22] did not provide the methodology of the study or the demographics of the participants. It is also not clear how many icons children need to select to create a password or how secure these passwords would be. Mendori et al. [22] did not test the new authentication method for security, usability or memorability. Further studies need to be conducted to develop a prototype and test it for security and memorability.

PassTiles is another graphical password system that could help users in authentication. It can be configured to retrieve information from memory using recognition, free-recall or cued-recall. Assal et al. [3] conducted a study to understand differences between children and adults authenticating using three PassTiles schemes. The three main variations of PassTiles used in the study are: Objects [34], Image [34], and Words [38] schemes. In any one variation, users are presented with a number of square tiles on a grid, and their password is composed of five random tiles selected by the system. To successfully authenticate, users have to choose these five tiles. In the Objects scheme, users are presented with tiles of images of different objects. In the Words scheme, users are presented with tiles of images of different words. In the Image scheme, users are presented with a background image with a grid superimposed on the image. Objects scheme leverages recognition and Image and Words scheme leverage cued-recall.

The study was conducted with 25 children and 25 adults. Both children and adults created passwords in each of the three PassTiles schemes. For each scheme, participants (children and adults) were asked to memorize system generated passwords. Participants were encouraged to practice inputting the password as long as it takes them to remember the password successfully. Participants (children and adults) were later asked to login to each of the three schemes at two different times. The results indicated that children process information differently than adults. Adults in the study used strategies to remember information that children might not have learned yet. For instance, in Word PassTiles scheme, adults linked words in a way to generate a story to help them memorize their password. Children and adults preferred the Object PassTiles scheme over the other two schemes and overall they preferred graphical passwords to their existing authentication scheme. The researchers found that children are unaware of security practices; due to which they put themselves at risk. These findings are similar to Read at al. [25] findings; they found that young children do not have good mental models privacy. Assal et al. [3] recommend that when designing authentication systems for children, we need to take into consideration their cognitive abilities and skills. They propose three design recommendations for authentication system designed for children: facilitate memorization through learning

and training features; adapt the interface to be age-appropriate for children; combine schemes to improve memorability (Objects and Images).

Based on the findings [9, 22, 34], it seems like graphical based authentication is better than text-based authentication. However, the variation of PassTiles that we discussed might not be ideal for children. Children had difficulty in remembering their passwords and took longer to memorize them compared to adults. Further research needs to be conducted to figure out the type of graphical authentication system that is best suited for children.

2.4 Alternative methods of authentication for children

There are limitations for both textual and graphical password systems, Renaud et al. [27] recommend a new authentication system based on cued-recall. Cued recall reduces the load on memory compared to recall as users' recall is aided by a cue. The new authentication system ("Little Bo Peep") has two steps: initialization (creating a password) and authentication. In the initialization step, users first select a theme from a list of options such as fairy tales, adventures, historical stories, westerns, and fantasies. The themes can be adjusted to reflect users' age (younger and older children). Users are then presented with queries related to the theme and a list of options. Users modify the details of the queries from list of the options presented to create a new and unique version of a story related to the theme. For example, if a user selected a "fairy tale" theme, they would be presented with a query such as "Cinderella married a PRINCE" and a list of options to modify the query. Users can modify the query to "Cinderella married a MONKEY" by selecting "MONKEY" from the list of options. Users are presented with several queries, and they modify them to make a story. The goal is to personalize the story to make it easier to remember. The story is stored as the users' password in their profile. During the authentication step, users select the theme they picked during the initialization step. They are then presented with the same queries and options as the initialization step, and they have to complete the story. If users' story matches with what is stored in their profile, they are granted access.

This method of authentication might be useful for children. Children would need

to recall the story based on the cues that are presented to them, instead of trying to recall the password without a cue. The authors claim that this new authentication system is secure and resolves many of the problem found in the text-based authentication system. We would need to build such an authentication system and conduct studies to test for usability, memorability, and security as well as compare it against text-based and existing graphical based authentication systems.

Chapter 3

Study 1 : Lab study of alphanumeric password rules

Children regularly use websites and applications that require an account to interact with them. Not all of these websites and applications have the same password creation rules. We are interested in finding out how children create passwords on websites with different password rules. To understand this, a study was conducted with children who were regular Internet users. The study was cleared by Carleton University's Research Ethics Boards (CUREB) #104813.

3.1 Study Design

3.1.1 Participants

The study was conducted with 20 participants between ages 11 to 13 years. 11 participants were female and 9 were male. Ten participants were 11 years old, six were 12 years old and four were 13 years old. Eleven participants were in Grade 6, five were in Grade 7 and four were in Grade 8. Participants were regular Internet users. 80% of them frequently downloaded applications from the Internet (on laptops, tablets or smart phones). 75% of participants created an account on these applications by themselves. For 25%, parents or a guardian created an account. Most participants (75%) logged into the applications or websites at least once a day and the remaining 25%, logged in at least weekly.

3.1.2 Methodology

Participants were recruited through social media (Facebook), friends and family. A poster about the study was posted on Facebook, online parent groups and family/friends were asked to distribute posters through email or in person to parents who would be interested in their children participating in the study. Participants

were compensated with a $15 Chapters giftcard.

Parents were given options on where they would like to meet to conduct the study: a public library, lab at Carleton university, or their home. For the study, the researcher needed a well-lit and quiet room with access to Wifi. Participants and their parents were greeted by the researcher, who thanked them for participating in the study. Parents were then given a parental consent form (Appendix A), which outlined how the study would be conducted and what their child needs to do to participate in the study. Parents read and signed the consent form apart from their child since it contained information about the study that the child should not know until the study was finished. Once the consent form was signed, the researcher read the assent form (Appendix B) to the child participant. The verbal assent form had information on how the study would be conducted and what participants would do. Participants were informed that they could ask to stop the study at any time and if they did they would still get the $15 Chapter's gift card. In the verbal assent form, we told the participant that we were testing usability of three websites. We did not tell them the real intent of the study, which was to understand how they create passwords. We believe that if participants knew that the researchers were interested in studying their password behaviour, they might have been more careful in the type of passwords they created.

The three websites used in the study were: "QuizMe", "FunZone", "OpinionMatters". These websites were created by us in Wordpress using various plugins and the MVP framework [8]. MVP logs users' activity on a website. This allowed us to collect data from each website, such as the passwords, password creation time, login time and users' errors during login. The "QuizMe" website (shown in Figure 1) asked participants to complete quizzes on three different topics. The "FunZone" website (shown in Figure 2) asked participants to play a game. The "OpinionMatters" website (shown in Figure 3) asked participants' opinion on five questions. The data was collected from each of the three websites and from the participants' responses to three questionnaires (demographic, during-test and post-test). The demographic questionnaire (Appendix C) asked questions about the participants: their age, gender, how many hours they spend online. The questionnaire conducted during the study (Appendix

D) asked participants what they thought of the website they just interacted with and how they created the password on that website. This questionnaire was short, with only four open-ended questions (what do you like or dislike about the website). The post-test questionnaire (Appendix E) asked participants about their experience with the three websites and what they thought about the passwords they created on these websites. The questions were a mix of multiple choice and open-ended. For each of the questionnaires, the researcher read the questions to the participant and wrote down their responses.

Figure 1: The "QuizMe" website used in the study

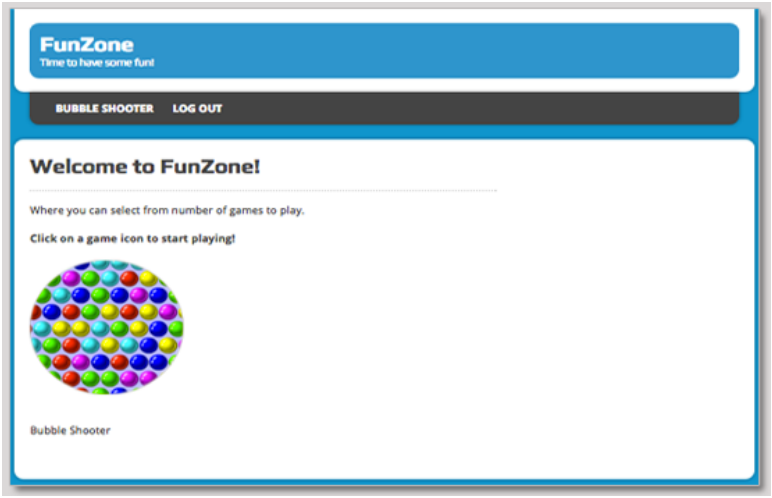

Figure 2: The "FunZone" website used in the study

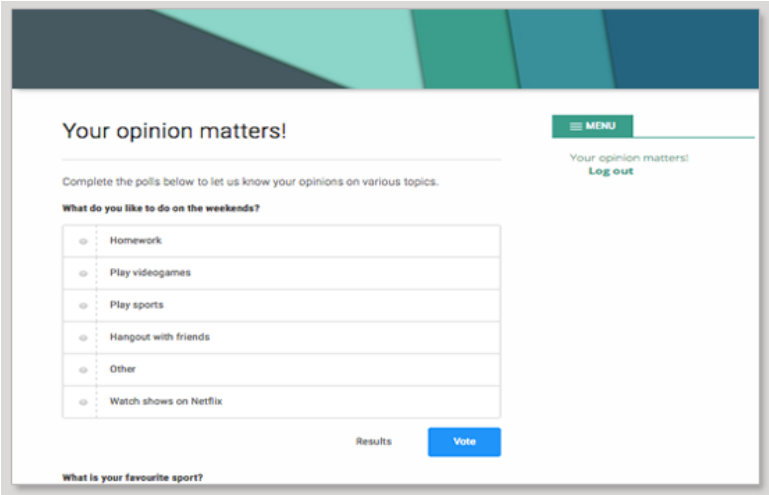

Figure 3: The "OpinionMatters" website used in the study

The researchers were interested in understanding the types of passwords participants create when they are presented with different rules. In the study, participants had to create a password, login and complete a task on each of the three websites. Each website had different password creation rules, as shown in Table 6, that varied in complexity. Password rules on the "QuizMe" website were of *low complexity*, "FunZone" were of *medium complexity* and "OpinionMatters" were of *high complexity*.

Table 1: Password creation rules

QuizMe	- minimum length of six	Low complexity
FunZone	- minimum length of six characters - at least one uppercase letter - at least one lowercase letter - at least one number	Medium complexity
OpinionMatters	- minimum length of six characters - at least one uppercase letter - at least one lowercase letter - at least one number - at least one special character (any character on a keyboard that is not a number or a letter)	High complexity

Upon participants' verbal confirmation that they wanted to participate in the study, participants were asked to verbally answer a demographic questionnaire as

Figure 4: Steps for each website; participants completed the cycle three times.

shown in Appendix C (e.g., age, gender, what grade they are in). The researcher recorded participants' responses on paper. Participants were then given a 15.5 inch HP touch screen laptop with Windows 10 operating system with the three websites preloaded in a web browser (Chrome) tabs. Participants were informed that they could use the touchscreen to interact with the website instead of the touchpad.

Latin square design was used for presentation order of the websites to ensure that order does not affect the results of the study. A username was provided to the participants at the beginning of the session. The same username was used for registering on all three websites. Figure 4 shows the steps that took place in the session. Participants registered on a website by creating a password and then logged in to that website. Once logged in, they completed a task, such as taking quiz, playing one level of a game, or giving their opinion on a few topics. Participants then logged off from the website and answered a brief questionnaire (Appendix D) on what they thought about the website and how they created the password. This cycle (Figure 4), registration, login, complete a task and answer a few questions repeated on all three websites. After which, the participants answered the post-test questionnaire (Appendix E) about their experience on interacting with the three websites and what they thought about the tasks that they had completed. Finally, participants logged in to each of the three websites again, in the same order as they logged in the first time. This was done to allow time to lapse between the first and second login attempt for each of the website.

The researcher debriefed the participants on the real purpose of the study, which was to understand their password behaviour. For the purpose of this study, the three

conditions that we are interested in from the study are passwords with *low complexity* ("QuizMe"), *medium complexity* ("Games") and *high complexity* ("OpinionMatters").

3.2 Results

The purpose of the study was to understand children's password creation behaviour with different password rules, such as passwords with *low complexity*, *medium complexity* and *high complexity*. We looked participants' password creation time, login time, recall, the types of passwords they created, and their strength.

3.2.1 Creation time

Creation time was measured in seconds, from the time participants clicked on the "Register" button until they successfully created an account. As shown in Figure 5, participants took longer (M=82.05, SD=32.27) to create passwords in the *high complexity* condition than *medium complexity* (M=36.40, SD=39.63) or *low complexity* (M=54.10, SD=15.94) conditions. In the *medium complexity* condition, there were two outliers, which could have impacted the mean of the results. Figure 5 also shows that the distribution in three conditions is positively skewed, therefore indicating that it took most participants longer than the median to create the password. The skeweness in the *low complexity* condition is 1.06, *medium complexity* is 1.57 and *high complexity* is 0.59.

A repeated measures analysis of variance (ANOVA) showed that the creation time significantly differed between the three conditions (*low*, *medium* and *high* complexity), $F(2,38) = 16.54$, $p<.05$. Pairwise tests using Tukey HSD showed that there was a significant difference in creation time between the three conditions. *Low* and *medium* complexity (p=.03), *medium* and *high* complexity (p=.01), *high* and *low* complexity (p=<.01), *high* and *medium* complexity (p=.01). Therefore, it seems like complexity of a password significantly increases creation time.

We grouped participants into three categories for the following analysis, based on which password rule condition they saw first. *Low-complexity-first* includes LMH (low, medium and high) and LHM presentation order, *medium-complexity-first* includes MLH and MHL, and *high-complexity-first* includes HLM and HML ordering.

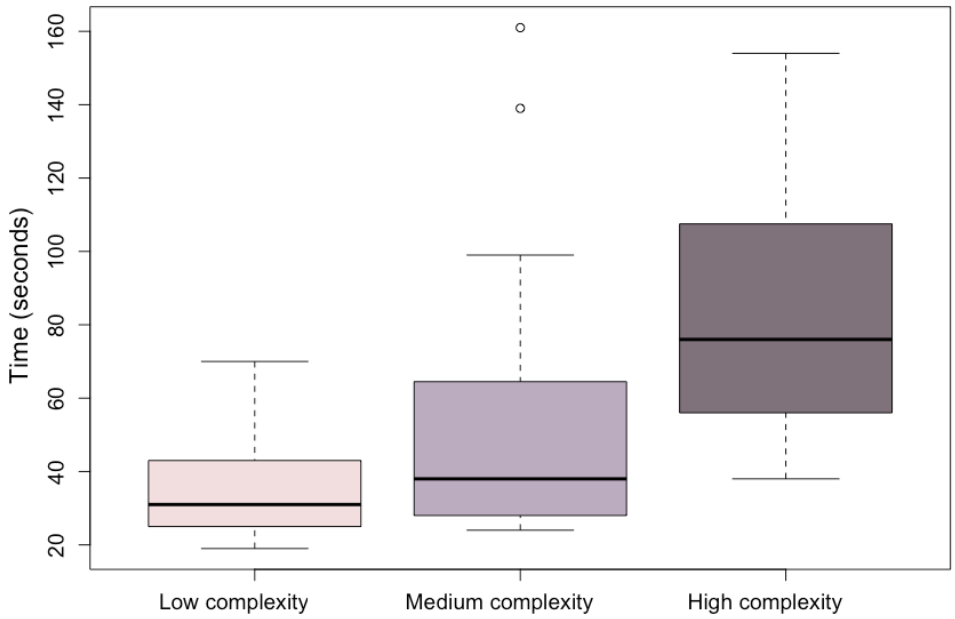

Figure 5: Boxplot of time in seconds it took participants to create passwords in each of the three conditions

We believe that participants who created a highly complex password first would reuse the same password in the other two conditions (*low* and *medium*); hence, reducing their overall password creation time across three conditions. The password rules in *low complexity* and *medium complexity* conditions were a subset of password rules in *high complexity* condition. Based on the Latin Square ordering, 7 participants first created a high complexity password, 7 participants first created a medium complexity password and 6 participants first created a low complexity password.

Figure 6 suggests that, overall, participants created passwords more quickly when they were first presented with the *high complexity* condition (M=50.33, SD=22.06) than *low complexity* condition (M=62.42, SD=29.57) or *medium complexity* condition (M=58.71, SD=17.87). Figure 6 also shows that there is a lot more variability in password creation time in *low-complexity-first* ordering.

To assess if there was a difference in creation time between the three categories of presentation orders, a repeated analysis of variance (ANOVA) was conducted. ANOVA showed that creation time did not significantly differ between the three presentation orders, $F(2,17)=3.02$, $p=0.08$. Therefore, the order in which conditions were presented to the participant did not affect their average password creation time

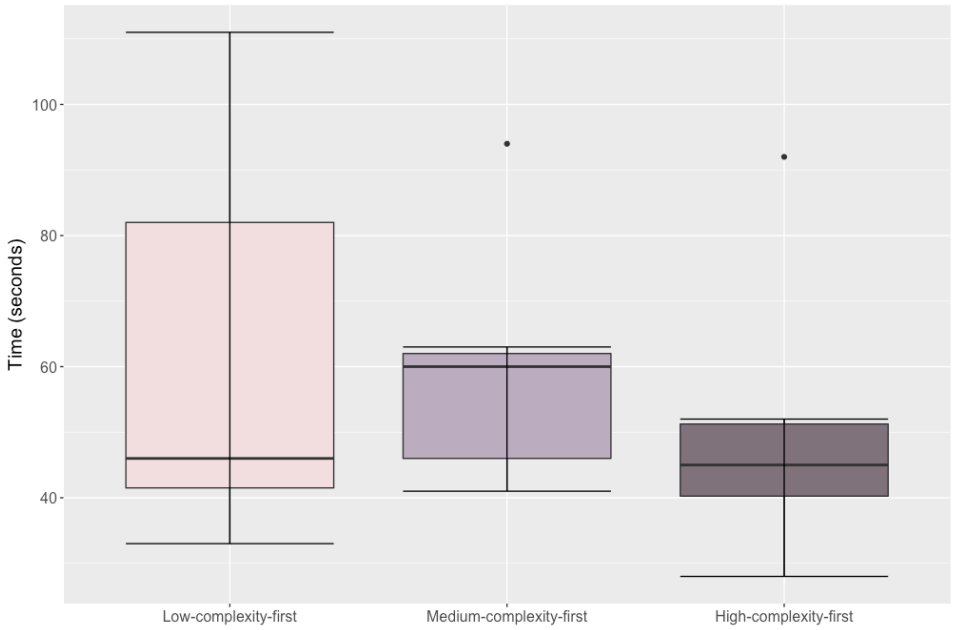

Figure 6: Boxplot of average creation times per user for different categories of presentation orders.

(across the three conditions). This could be because four out of seven participants who first created a highly complex password kept the exact same password for the other two conditions.

3.2.2 Login time

Participants had to login twice to each website. They first logged in after creating each password and then again at the end of the study. Login time was calculated from the time the participants clicked on the "Enter your password and login" button to until they were successfully logged into the website. Some participants did not make any error during login while others made a few errors. The login time for a participant who made several errors would be higher compared to participants who made no errors which would skew the results. Therefore, the login time did not include the time it took participants to re-enter the password if they made an error. Errors included misspelled words, extra/incorrect number of spaces or typos. Login time included the total time participants took to successfully login (last login) to a website without making an error.

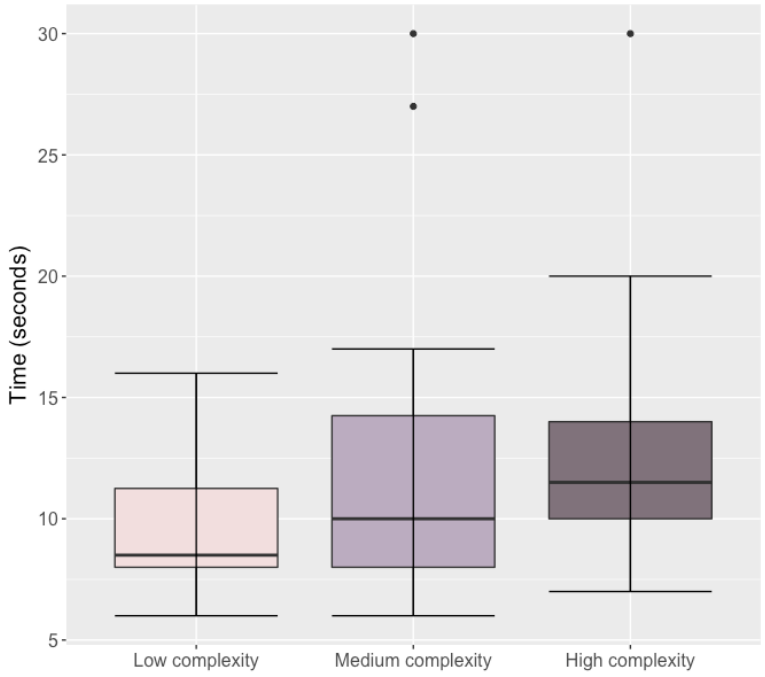

Figure 7: Average login time per participant of both login attempts in each of three conditions

Figure 7 shows an average login time in seconds across two logins for each of the three conditions (*low*, *medium* and *high* complexity). Figure 7 suggests that participants took slightly longer to login in *high complexity* condition (M=12.85) than *low* (M=9.55) or *medium* (M=11.95) complexity conditions.

To assess if there was a difference in average login time between the three conditions (*low*, *medium*, *high* complexity), a repeated analysis of variance (ANOVA) was conducted. ANOVA showed that login time did not significantly differ between the three conditions, $F(1.69,32.03)=2.54$, $p=0.10$.

There was a time lapse between the first and second login attempt. We were interested in finding if there was a difference in login time between these two attempts. As shown in Table 7 and Figure 8, it took participants slightly longer to login during the second login attempt.

A repeated two-way analysis of variance was performed to determine the effect of two variables (login attempt and password complexity) on login time. Login attempt consisted of two levels (first, second) and password complexity consisted of three levels (low, medium, high). There was no statistically significant difference found

Table 2: Mean and standard deviation of login times for the first and second login attempt in seconds

Password complexity	**First login**		**Second login**	
	Mean	**SD**	**Mean**	**SD**
Low	8.95	3.63	10.00	4.31
Medium	11.60	8.27	12.50	9.27
High	11.75	7.68	13.65	6.39

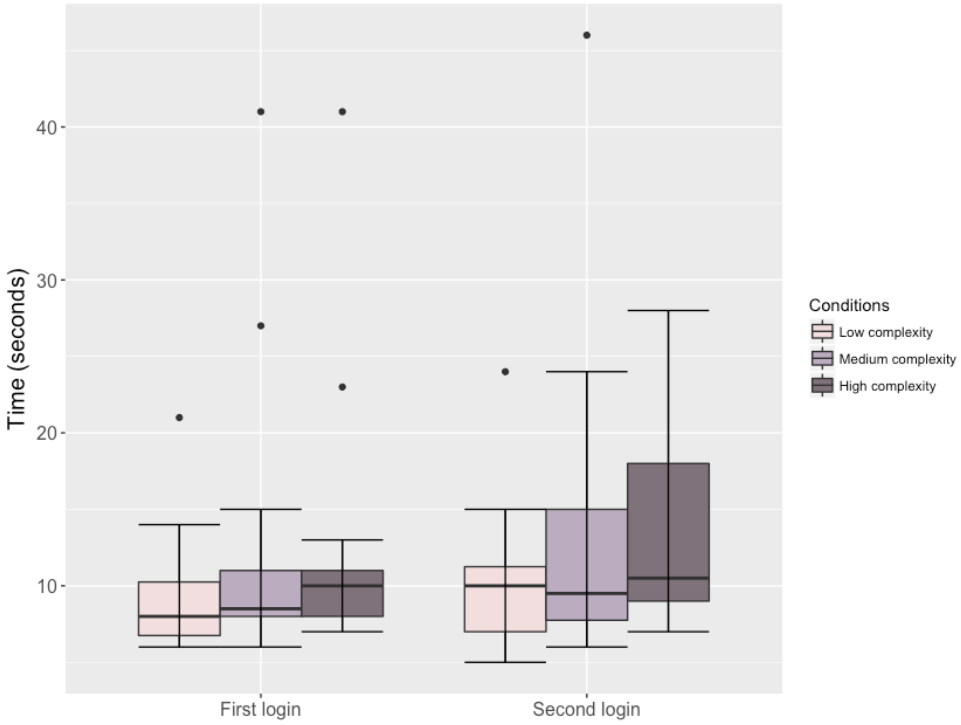

Figure 8: Login time of first and second login attempts in each of three conditions

for the main effect of login attempt ($F(1,19)=2.30$, $p=.15$), indicating there was no difference in login times between the two login attempts. There was also no statistically significant difference found for the main effect of password complexity, ($F(2,28)=2.69$, $p=0.08$), indicating no difference in login times between the three conditions across the login attempts. Also, the interaction effect between the login attempts and password complexity was not significant, $F(2,38)=0.05$, $p=.95$.

3.2.3 Recall

In the post test questionnaires, participants reported that they remembered their password in all three conditions for the duration of the study. Twelve participants successfully logged in during both login attempts without any failures. However, eight participants had difficulty recalling their password during the first or the second login attempt.

Participants tried to login until they were able to recall their password. Failures were incremented every time a participant entered an incorrect password during login. Four participants accounted for the 6 failures during the first login attempt. From these four participants, two had 1 failure each and two had 2 failures each. Six participants accounted for 8 failures during the second login attempt. From these participants, four had 1 failure each and two had 2 failures each. Most of the failures occurred during the second login attempt. As shown in Figure 9, *medium complexity* and *high complexity* conditions had the most failures. A repeated analysis of variance showed that there was no significant difference in number of failures in the three conditions (*low*, *medium* and *high* complexity), $F(2,38)=2.04$, $p=0.15$.

In most failures, the password entered by the participant was closely related to their actual password. Participants made small errors during login, for example, they forgot to hold down shift key for special character (entering 2 instead of @), accidentally pressed on the caps lock key (entering "HMJT05!" instead of "Hmjt05!"), misspelled a word (entering "watermeon" instead of "watermelon"). There are two types of user errors; mistakes and slips [23]. Norman [23] refers to "slips" as users intending to do one action but end up doing another and "mistakes" as users' intention to do something being incompatible with the action they are trying to achieve. For example, users clicking on the "print" button to save and print their file when it does not do that. The "print" button only prints their file without saving it. Slips often occur when users are familiar with how to complete a task but accidentally do something different. In our study, participants had slips rather than mistakes. This suggests participants did not forget their password, but they made errors in entering it.

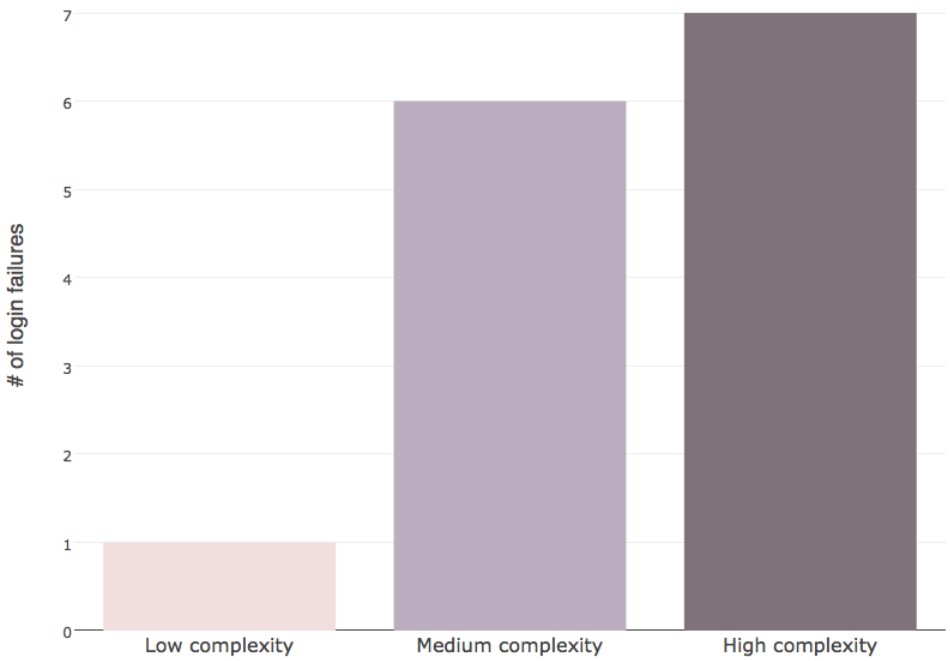

Figure 9: Total number of login failures in each of the three conditions across both logins

3.2.4 Passwords

From the questionnaires (during and post-study), we found that 55% of participants used their personal information to create the passwords. Personal information included name, nickname, family pet's name, date of birth. Six participants reported that they created random passwords for the duration of the study, four participants reported that they used their actual password and ten participants reported that they used parts of their actual password.

Figure 10 suggests that participants felt it was most difficult to create passwords in *high complexity* condition compared to other conditions. Participants reported that this was due to the number of rules required to create a password in *high complexity* condition. Two participants (one in *low-complexity-first* order and the other in *medium-complexity-first* order) reported that they had most difficult in creating passwords in the first condition presented to them, regardless of which condition. This was because they had to think and come up with a password, which they could later reuse in other conditions. One participant reported that they had the most difficulty

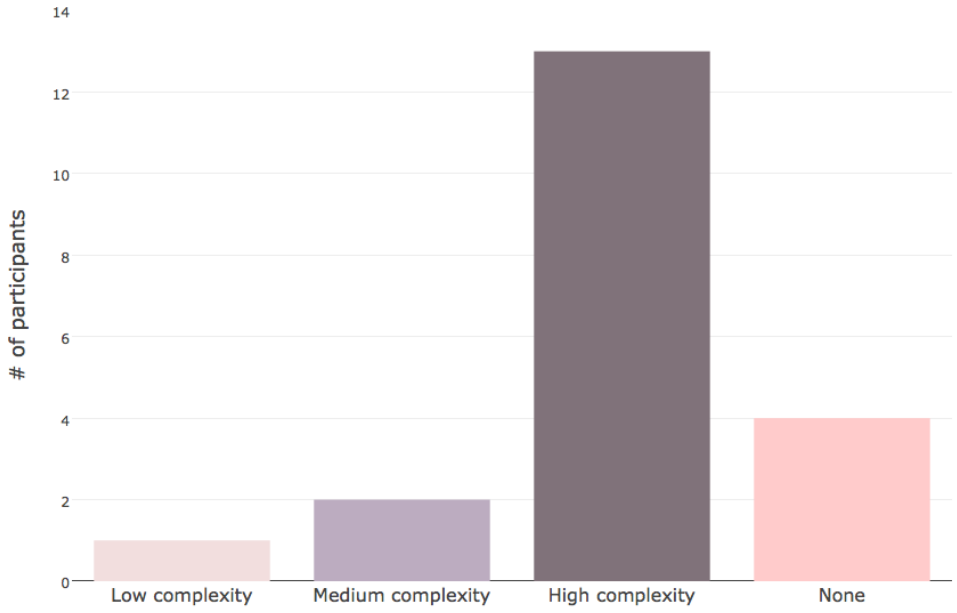

Figure 10: Condition in which participants found it most difficult to create the password

in creating a password in *medium complexity* condition because they misunderstood the password rules. The participant thought that the password length needed to be exactly six characters. If they had known that the password could be more than six characters long, they would have created the same password in all three conditions. Four participants reported that they had no difficulty in creating passwords in any of the three conditions because they created it once and used the same password in the other conditions.

Password reuse

Seven participants out of 20 (35%) used the exact same password in at least two conditions and their password in the third condition was similar to the first two. For example, a participants' password in the *low complexity* condition was "Welcome2EV", the *medium complexity* condition was "Welcome2EV" and the *high complexity* condition was "Welcome2EV!". The other thirteen participants' passwords also had similarity across conditions. The first part of a password was same and the remainder of each password was modified to meet the password rules specific to the

condition. For example, a participants' password in the *low complexity* condition was "blanc111", the *medium condition* complexity was "Blanc111" and the *high complexity* was "Blanc111!". Others had two passwords with high similarity and one that was unique.

Special character

Passwords created in the *high complexity* condition required at least one special character. Participants were not told in advance what is considered a special character. From the data collected through the interviews, 10 participants reported that they did not know what a special character was during password creation. The researcher had to tell them that it was "anything that is not a number or a letter" before they could create their password. From these 10 participants, 7 were of age 11, 2 were of age 12 and one was of age 13. Most twelve and thirteen year old participants knew what a special character was, but, most eleven year old participants did not. Eleven participants included an exclamation mark (!) in their password, three used an @, two used an underscore(_), and the remainder each used a unique symbol ($,*,#,.). Only four participants used special characters in conditions where it was not mandatory.

Password Strength

In the post-test questionnaire, participants were asked if they thought that a stranger would be able to guess the passwords they created in the study. As shown in Figure 11, most participants in each condition believed that their passwords would not be easy for a stranger to guess. Among those who were less confident in their password, participants believed that some of the passwords were too simple and contained their personal information, such as name or age.

Most participants (N=16) did not want anyone including their siblings or friends to have access to their account. From the 16 participants, 2 did not even want their parents to have access to their accounts. The other 14 participants did not care if their parents had access. Participants' main concern was privacy; they did not want anyone else to have access to their personal information. For siblings, their main concern was that they would "mess" with their account.

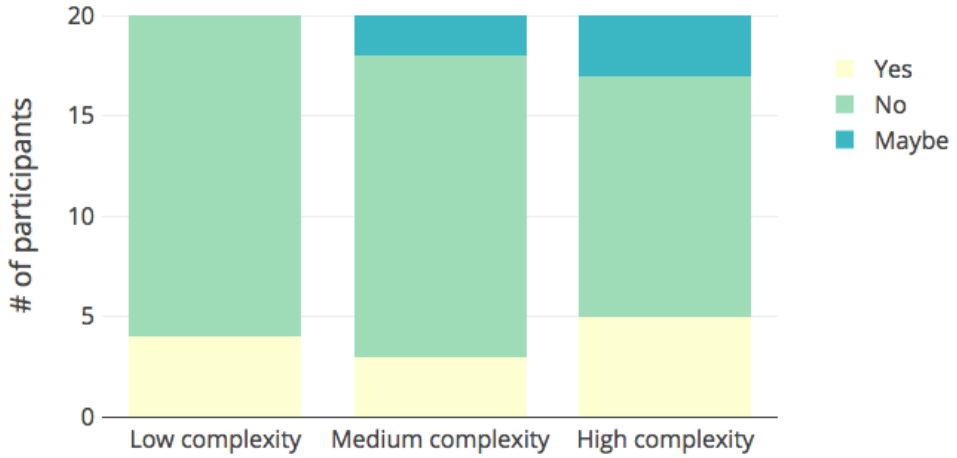

Figure 11: Participants' response for question "Do you think it would be easier for a stranger to guess the passwords?"

A password's strength depends on several factors, such as its length, character set, and the presence of words in the password. Several password policies and guidelines recommend how to create strong passwords. For example, the 2017 NIST guidelines [15] recommend that passwords must be at least eight characters long and should not include known compromised passwords, commonly used words, dictionary words, or contain repetitive/sequential characters.

Generally, a password's strength is measured by its complexity and length. The complexity of the password increases based on the number of character sets used (lowercase letters, uppercase letters, digits, and symbols). A password's entropy [31] is a measure of strength based on its length and the character set (entropy is measured in bits). Longer and complex passwords have a higher entropy than short and simple passwords. Passwords with higher entropy are able to sustain a brute force guessing attack better than passwords with lower entropy. Using NIST's [5] recommended Shannon's entropy formula [31], we calculated the entropy of passwords created in the three conditions. Figure 12 shows the resulting entropy of passwords: *low complexity* (M=57), *medium complexity* (M=57) and *high complexity* (M=59). A repeated analysis of variance with Greenhouse-Geisser correction showed that there was no statistically significant difference in password strength between the three conditions, $F(1.26,29.93)=.32$, $p=0.63$.

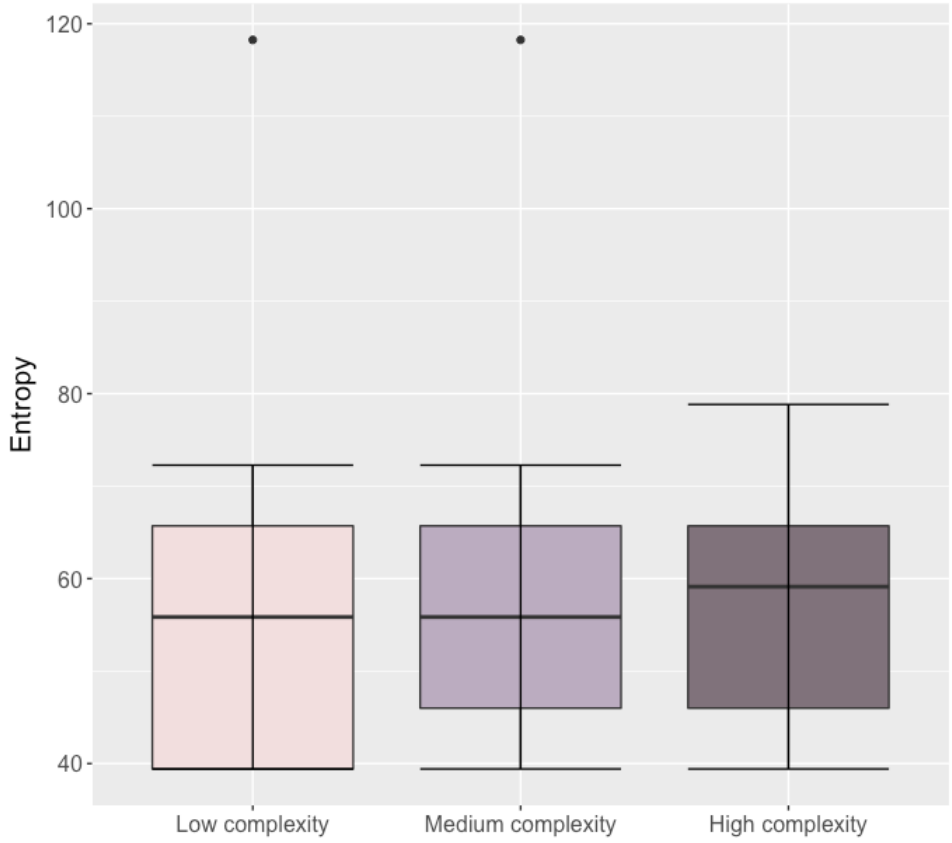

Figure 12: Shannon's entropy of each passwords in three conditions

Entropy does not take into account dictionary attacks, commonly used words or pattern of characters in a password. For example, "Welcome2EV" password has higher entropy (66 bits) than the password "Hmjt05" (39 bits), even though the first password contains a dictionary word, hence is more prone to dictionary attack.

Although there was no difference in entropy between the conditions, we believe that there is a difference in strength. A password composed of commonly used words is not as strong as a password that is randomly generated and does not contain personal information or dictionary words. Following some of the NIST guidelines, we subjectively assessed passwords on scale of 1 (least secure) to 5 (highly secure). The scale takes into account a password's length, complexity, vulnerability to dictionary attack, inclusion of commonly used words and use of repetitive/sequential characters (e.g, "123"). Table 5 shows the score for five sample passwords.

Based on this new password criteria, two researchers independently scored each

Table 3: Password strength scores assigned to sample passwords

Password	**Score**	**Strengths**	**Weaknesses**
kylese	1	- none	- contains participant's name - only composed of lowercase characters - does not contain a special character - does not contain a number
Jame16	2	- contains mix character case - contains numbers	- contains participant's name - does not contain a special character
Stella123$	3	- contains mix character case - contains numbers - contains a special character - length is greater than six	- contains participant's name - commonly known digit sequence at the end
cS9333*	4	- random password - contains mix character case - contains numbers - contains a special character - length is greater than six	- contains a predictable number pattern
Hmjt05!	5	- random password - contains mix character case - contains numbers - contains a special character - length is greater than six	- none

of the passwords in the three conditions. A weighted Cohen's Kappa(κ) test showed moderate agreement between the two researchers' ratings of password strength (k=0.54, p <.01). Table 4 lists out interpretation of different values of Cohen's Kappa [19]. The researchers' scores were averaged to get a strength score for each of the passwords (Appendix F). Some of the passwords in the study were participants' real passwords and others contained their name. Therefore the passwords in Appendix F are similar to the passwords participants created in the study, but have been modified to protect participants' personal information.

As shown in Figure 13, passwords in the *low complexity* condition range from 1 to 3 (M=2.15), those in the *medium complexity* condition range from 2 to 4 (M=2.85) and those in the *high complexity* range from 3 to 5 (M=3.45). A repeated measures

Table 4: Description of different values of Cohen's Kappa(κ)

κ<0	Poor agreement
$0.0 < \kappa < 0.20$	Slight agreement
$0.21 < \kappa < 0.40$	Fair agreement
$0.41 < \kappa < 0.60$	Moderate agreement
$0.61 < \kappa < 0.80$	Substantial agreement
$0.81 < \kappa < 1.00$	Almost perfect agreement

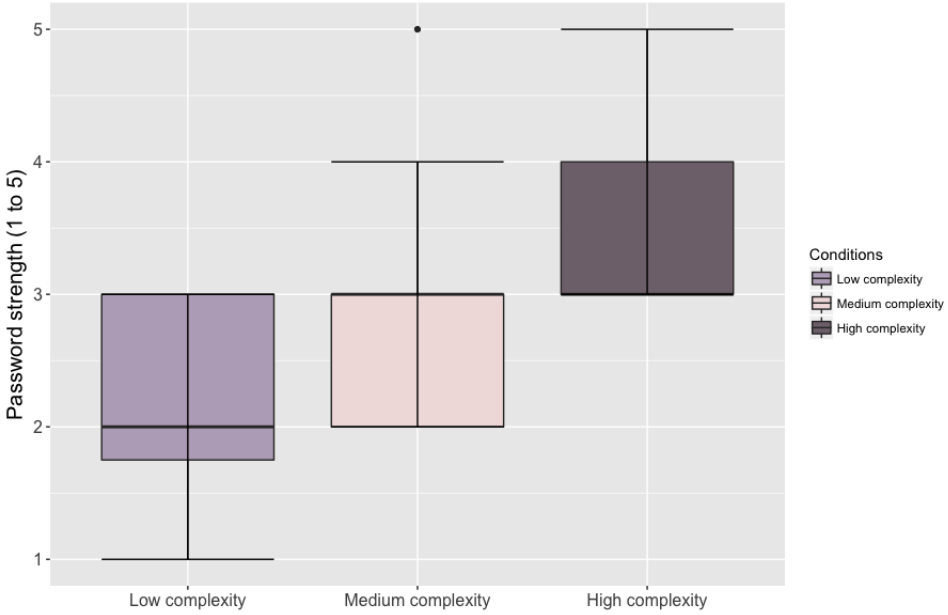

Figure 13: Password strength on scale 1 (weakest) to 5 (strongest) for password in the three conditions.

analysis of variance showed that there was a statistically significant difference in password strength between the three conditions ($F(2,38)=20.45$, $p<.01$). Pairwise post hoc tests using Tukey HSD correction showed that password strength significantly differed between all three conditions ($p<.01$).

3.3 Discussion

In our study, participants interacted with three different websites with different password creation rules. We were interested in finding out how participants create passwords on these websites. The key findings from the results of the study are: children

created simple passwords that are easier for them to remember; they reused a password on multiple websites; they did not find it difficult to create passwords with different password rules except one (special character rule); they created passwords longer than minimum password length of six, and they believed that they created secure passwords. We also subjectively assessed passwords' strength by taking into consideration their character set, length and the words used in the password. In the sections below we will go through the each of the key finding in detail.

Password creation

The results of the study indicated that participants had no trouble creating passwords with most rules except the special character rule. Some participants (N=11) created simple passwords using their personal information. We believe that participants used their personal information to create passwords so that they are easier for them to remember. Children might have learned this method of creating the password from their parents or a guardian. Similar finding were reported by Zhang-Kennedy et al. [40], where they found that younger children (ages 7 to 11 years) were encouraged by parents to create simple and easy to remember passwords. Parents could also teach their child to create simple and easy to remember passwords so that they do not have to reset the password every time the child forgets his/her password.

Most participants (N=13) found it more difficult to create passwords in the *high complexity* condition compared to other two conditions because of the number of rules. Participants had difficulty with the special character in this condition; this could be the reason they found it difficult to create the password. Most participants (N=15) in the *low complexity* condition created passwords with similar rules as in the *medium complexity* condition even though they only had to follow one rule (length has to be at least 6 characters). This is most likely because participants are very familiar with the rules used in the *medium complexity* condition from their previous real life experiences. The rules in *medium complexity* condition are most likely similar to those on the websites with which participants often interact. Overall, we found that even with minimum password rules, children created passwords that included uppercase characters, lowercase characters or numbers. From these findings, we believe that

password rules for children ages 11 to 13 could reasonably include: mixed character case, numbers and a length of at least eight characters.

Most children in our study did not know about special characters. We believe that password rules for children ages 11 to 13 can include the special character rule if it is explained to them. Children need to be taught what is considered as a special character and how it can be include in their passwords (pressing shift and another key on the keyboard). A design recommendation in the literature for systems designed for younger (7 to 8 years old) children [26] is to require shorter passwords (4 to 8 characters with 4 being enough). Children in our study were much older (11 to 13 years old) and they created passwords longer than minimum required length (6). The average length of a password across the three conditions was nine, indicating that children are used to creating passwords longer than six characters. However, they might not be able remember long and complex passwords that do not contain their personal information.

Password memorability

Most participants recalled their password in all three conditions during first and second login. In the first login attempt, participants immediately logged into the website after creating the password and were easily able to recall their password. The second login attempt occurred at the end of the session. It took participants about 30 minutes to complete the session; they remembered the password for the duration of the session. There was not a significant time lapse between the first and second login. A longer time lapse might make a difference since participants would not be actively thinking about the password.

Participants who were not able to recall their password in the first attempt made minor mistakes in entering their password. These mistakes (failures) fell into several categories; they either entered a password that they had created for another condition, misplaced some characters of the password ("Ds34!ter" instead of "Ds34ter!"), forgot a character of their password ("Dsds56" instead of " Dsds456") or made a typo ("watermeon" instead of "watermelon"). The failures were due to participants making small errors and not because they completely forgot the password. Some participants

reported they had used their real password in the study and would remember it even after the study. Others reported that they created a random password for the study and they would not remember the password after a week or two.

Cole et. al [9] found that children's (ages 6 to 12) recall success rate fell from 100% to 84% after a two week time lapse. Further studies need to be conducted with children to test for long term memorability of passwords and figure out which password rules are best suited for children. Lamichhane et al. [18] found that children (ages 7 to 8) had difficulty recalling complex passwords during the first login attempt after a short period of time. Children in our study did not have difficulty recalling their password for duration of the study. This could be because children in our study were older or there was not significant time lapse between password creation and login in our study. It took participants an average of 30 minutes to complete the study.

Password strength

Participants were concerned about the safety of their accounts. They did not want strangers, friends, or siblings to have access to their account. Their main concern with strangers and friends was privacy. But with siblings, it was that they would "mess up" their accounts. This is somewhat similar to findings of Zhang-Kennedy et al. [40], where they found that childrens' perception of potential threat was their friends and siblings because they could "mess-up" their games or do things that could get them in trouble with parents. However, in our study, children's perception of potential threat also included strangers and their concern was them having access to their personal information.

As discussed in the results, we subjectively assessed the passwords, taking into account the character set as well as dictionary/common words and repetitive/sequential characters. We found that passwords in the *high complexity* condition were strongest, followed by these in the *medium complexity* condition and then those in the *low complexity* condition. We provide guidelines but relied on researcher making an assessment of password strength. Although different factors are taken into account when making the assessment, it is subjective. We had two researchers independently assess the passwords and found that there was a moderate agreement between their ratings.

Most participants (N=15) believed that the passwords they created would be difficult for a stranger to guess even though their password contained their personal information (name) and/or dictionary words. Participants created 60 passwords in the study across three conditions. These password were assessed and only 15 passwords scored between 4 (N=13) and 5 (N=2). Most of the passwords scored between 1 to 3. Therefore, participants thought that they created secure passwords when they did not. This suggests that children do not have the knowledge of what constitutes a strong password, at least accordingly to our criteria.

Conclusion

We now understand that children created simple passwords and that children think that these passwords are hard for a stranger to guess. Based on the results of our study, we recommend that children should to be taught at an early age how to create strong password so they are able to better protect themselves online. We also recommend that password creation rules for children of ages 11 to 13 should consist of numbers, mixed case characters and a minimum length of eight characters.

Anecdotally, we suspect that children are learning to create simple and weak passwords from their parents/guardians. In order to understand this, further studies need to be conducted with parents to understand their knowledge of secure passwords and what they teach their children about creating secure passwords. We also need to create strategies to teach children how to create secure passwords, come up with password design guidelines for systems designed for children and test for long term password memorability using these guidelines.

Limitations

The main limitations of the study were the duration of the study for testing password memorability and the ecological validity. Children created passwords on three different websites with different rules in an experimental setting. In real life, children most likely do not create passwords one after another in such a short timeframe, hence, reducing the chances of using the exact same password across different websites. They also have more time to think about creating a password and may ask their parents for

help in creating the password. During the study, children might have created random passwords since they did not have to remember them after the study. In real life, children might create more meaningful passwords that are easy for them to recall. Further studies need to be conducted to test for password memorability while trying to increase the ecological validity of the study (e.g., test one website with a rule at a time and have participants recall the password at a later time). Another possible limitation is the sample size used in the study; a large sample may have revealed other patterns. Despite these limitations, our study does provide insight in how children of this age group understand password rules and the strategies they take to meet these rules.

Chapter 4

Study 2: Evaluating parents' awareness of security and their children's password behaviors

The results of the first study indicated that children create weak passwords that are easy for them to remember. We speculated that children might have learned this method of creating passwords from their parents or a guardian. To understand parents' influence on children's security habits we conducted another study, with parents.

4.1 Study design

In this study, we are interested in understanding parents' knowledge of creating secure passwords, what they think about their children's password practices and the strategies they teach their children about creating secure passwords and staying safe online. The study was cleared by Carleton University's Research Ethics Boards (CUREB), REB clearance #107059.

4.2 Survey structure

The survey was designed by using the Qualtrics[1] online survey tool. It consisted of 55 questions divided into four sections listed below. Most of the questions in the survey were presented in Likert scale format (1 as strongly disagree to 5 as strongly agree) with a few questions presented in an open-ended format. Appendix I has a complete list of questions using in the survey.

The major sections were:

1. Demographic related information about the parent and the child

[1]https://www.qualtrics.com/

2. Parents' awareness of security cues and their password creation practices

3. Knowledge about the child's password practices

4. Parents' belief and practices about creating passwords and practicing safe online behaviors

The survey consisted of questions from the Security Behavior Intentions Scale (SeBIS) [12] to understand parent participants' level of awareness and their password creation practices. The SeBIS scale can be used to predict users' security behaviors [11]. From the SeBIS scale, our survey included 5 questions from the proactive awareness sub-scale and 4 questions from the password generation sub-scale. These questions were scored on a 5-point Likert scale. The scores for proactive awareness and password generation were calculated by taking an average of participants' response to the questions in each of the sub-scales. The SeBIS scale suggests that participants testing high on the awareness sub-scale are able to identify a phishing website successfully, and participants testing high on the password generation sub-scale create passwords that are hard to crack (secure passwords) [11].

The remainder of the questions were created by us specifically for this survey. We iterated them through several rounds within our research group and pilot tested with family and friends. We edited them for clarity based on the feedback.

4.3 Method

To complete the survey, parent participants read the online consent form and agreed to participate in the study. In the consent form, participants were informed that they could end the study at any time, but they would only be compensated if they completed the survey. After agreeing to participate in the study (Appendix G), participants answered a few pre-screening questions and then filled out the survey. Participants were given an option not to answer a question if they did not feel comfortable. They could either select "prefer not to answer" or leave a text field blank. The data in the study was collected from participants' responses to the questions in the survey.

4.4 Participant recruitment

Participants were recruited by Qualtrics based on the requirements provided by the researcher (Appendix H). Only, participants who met the study's requirements were allowed to complete the survey. The study's requirements were: participants must live in Canada, have a child between ages 6 to 13, and the child must be a regular Internet user. We were interested in understanding differences between parent participants' based on the child's age. Therefore, Qualtrics recruited at least 25 participants with a child in each of the four age groups: 6-7, 8-9, 10-11, and 12-13. In cases where parents had more than one child fitting the criteria, they were asked to reply to the survey only about one specific child.

Participants were compensated by Qualtrics once they completed the survey. Participants were compensated in various ways, such as SkyMiles, gift card, or points. The compensation was equivalent to $1.25 USD; this amount was set by Qualtrics based on their usual rates given the required demographics and the length of the survey. We paid Qualtrics $5.50 USD per participant for recruitment.

4.5 Participant demographics

The study was completed by 105 participants, 61% were mothers, 37% were fathers, and 2% were the child's guardian. Participants' age ranged from 21 to 60 years old, with a mean of 38 years old. 36% of the participants had one child, 39% had two children, and 25% had three or more children. Figure 14 summarizes the parent participants' education level; 81% had education beyond high school. 66% of the participants reported fewer than nine accounts for online applications or websites and 44% of participants reported having more than ten accounts. Parent participants spend an average of seven hours a day online.

As shown in Figure 15, children's ages ranged from 6 to 13 years old with as equal number of children in each of the age group. 81% of the participants reported that their child personally has an account on online websites and applications.

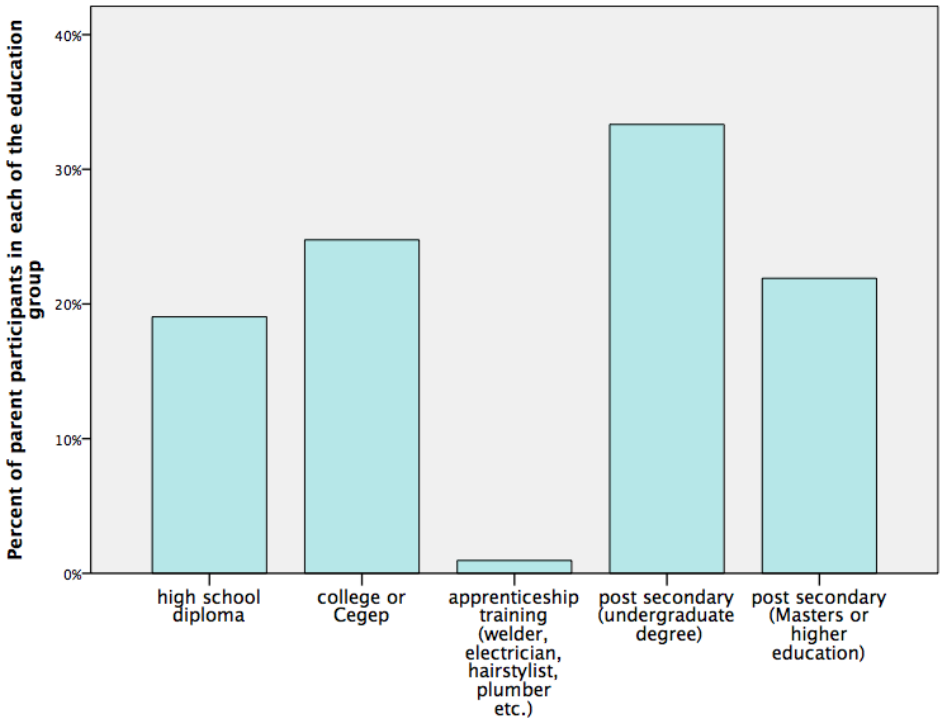

Figure 14: Parent participants' education level

4.6 Results

In this section, we will present findings from the survey to understand parent participants' awareness of security cues, password practices, parent participants' concern for their child's safety when they are online, and parent participants' beliefs and practices about creating secure passwords and practicing safe online behaviors.

4.6.1 Parents' awareness of security cues and their password creation practices

The survey included five question from the SeBIS scale [12] to measure participants' level of awareness of security-related cues. We calculated a participant's *proactive awareness* score by taking an average of their responses to the five questions. The *proactive awareness* score ranged from 1 (least aware) to 5 (highly aware). As shown in Figure 16, most participants' *proactive awareness* score was between 3 and 4 with only 14% of the participants scoring a five. Based on this, we believe that most

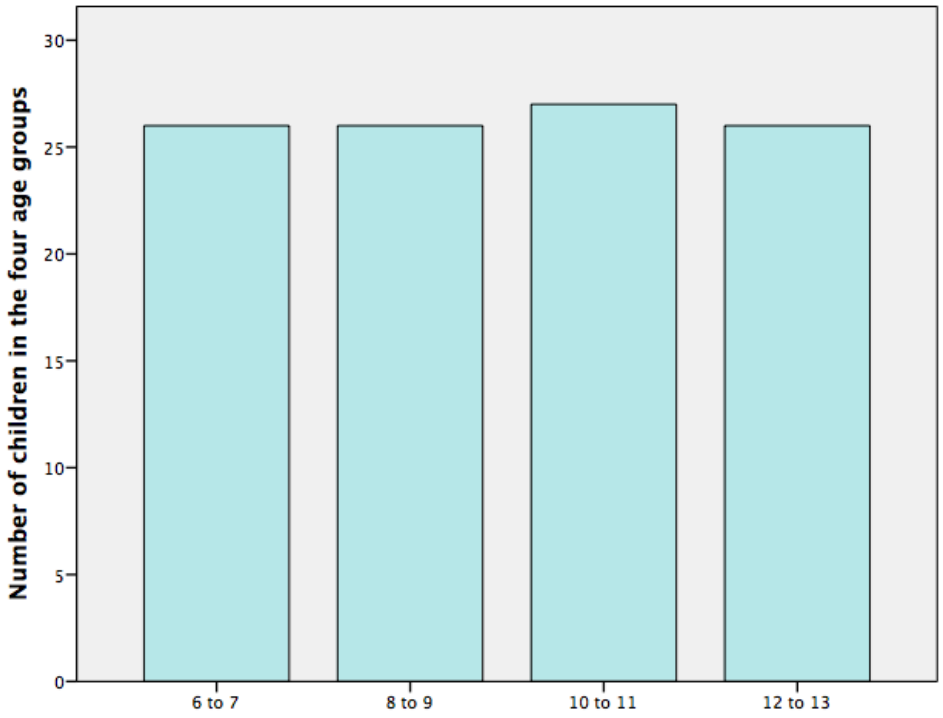

Figure 15: Number of children in each of the age groups (6 & 7, 8 & 9, 10 & 11, 12 & 13 year olds)

participants are somewhat aware of security cues and they will most likely detect a phishing website.

The survey also included four questions from the SeBIS scale [12] to understand participants' password generation behaviors. We calculated a participant's password generation score by taking an average of their responses to the four questions. The password generation score ranged from 1 (least secure) to 5 (highly secure). As shown in Figure 17, only 10% of participants scored a 5 and most participants (46%) scored a 3. Based on this, we believe that most participants will create "somewhat secure" passwords and only a few will create secure passwords (hard to crack).

As shown in Figure 18, 82% of parent participants reported that they have more than one password. However, as show in Figure 19, 38% of the parent participants also reported that they only have one password that they re-use across multiple websites. We believe that inconsistency in parent participants' response to the two questions ("I have more than one password for different websites" and "I only have

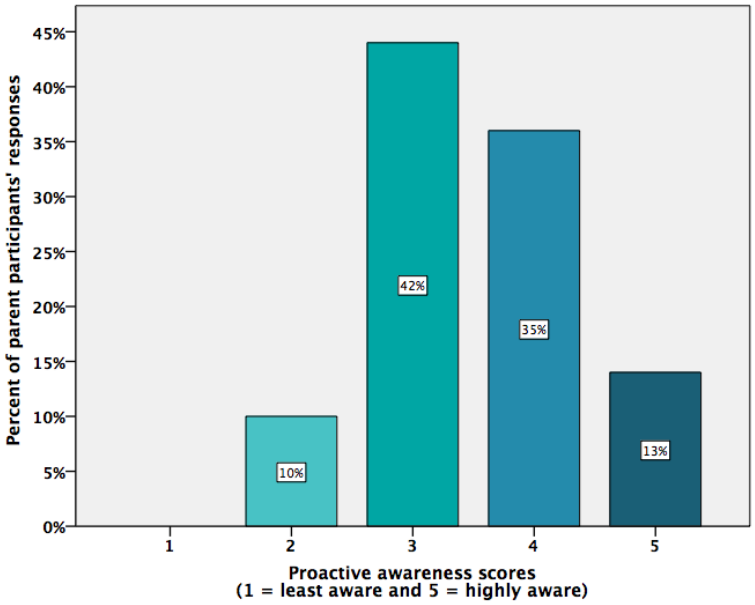

Figure 16: Participants' proactive awareness scores.

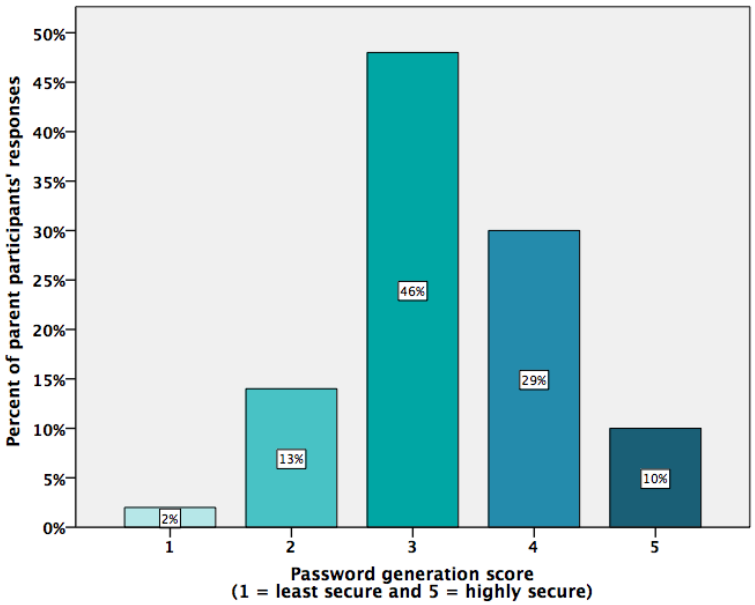

Figure 17: Participants' score for password generation behavior

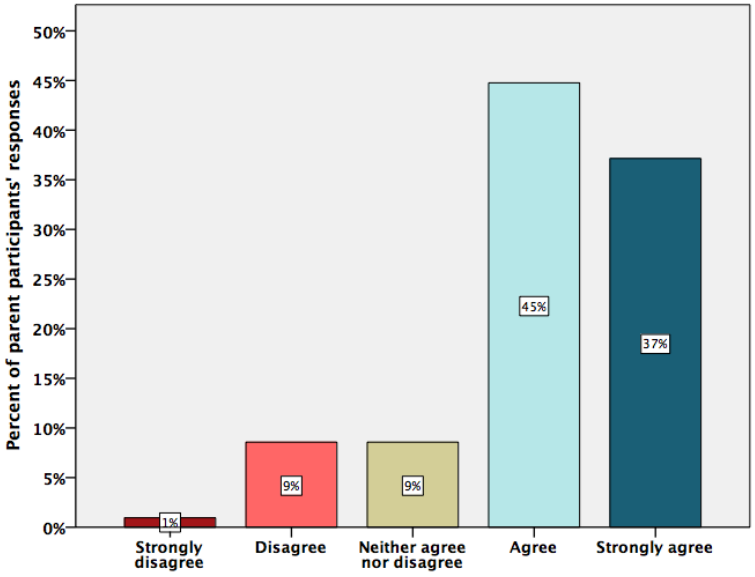

Figure 18: Parent participants' response to question "I have more than one password for different websites"

one password which I reuse across multiple websites") is due to the wording of the questions. Participants could have more than one password but also reuse one of their many passwords across multiple websites.

Participants scored five passwords from least to highly secure. Four passwords were taken from the ones children created in the first study. The five passwords were: "WelcomeDEV2", "P@ssword!", "987654321", "camila", "Hmjt05!". As shown in Figure 20, participants reported "camila" as the least secure and "Hmjt05!" as the most secure password. We subjectively assessed the strength of these passwords as we did in Chapter 3. The passwords scored as: camila(1), 987654321(2), P@ssword!(3), Welcome2DEV(4), Hmjt05!(5). Parent participants' assessed the password strength somewhat similar to our own subjective assessment. They scored the passwords in the order from least to highly secure as: camila(1.77), 987654321(2.50), P@ssword!(3.11), Welcome2DEV(3.38), Hmjt05!(4.16). This suggests that parent participants had a good understanding of "secure" passwords.

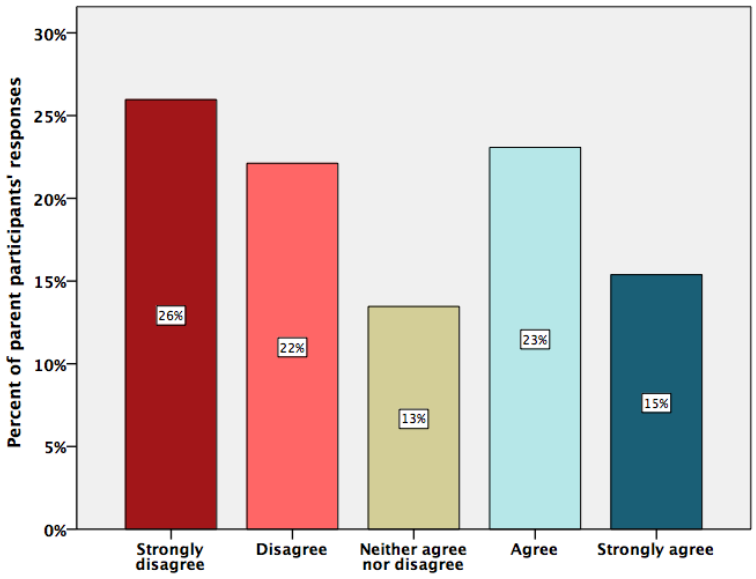

Figure 19: Parent participants' response to the question "I only have one password which I reuse across multiple websites"

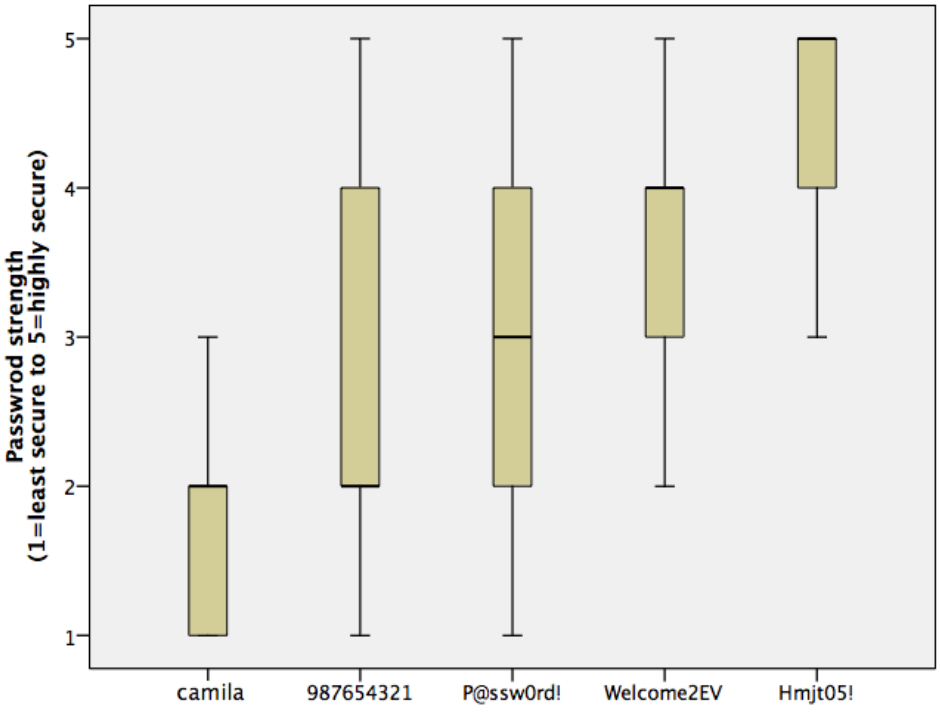

Figure 20: Parent participants' rating strength for five different passwords.

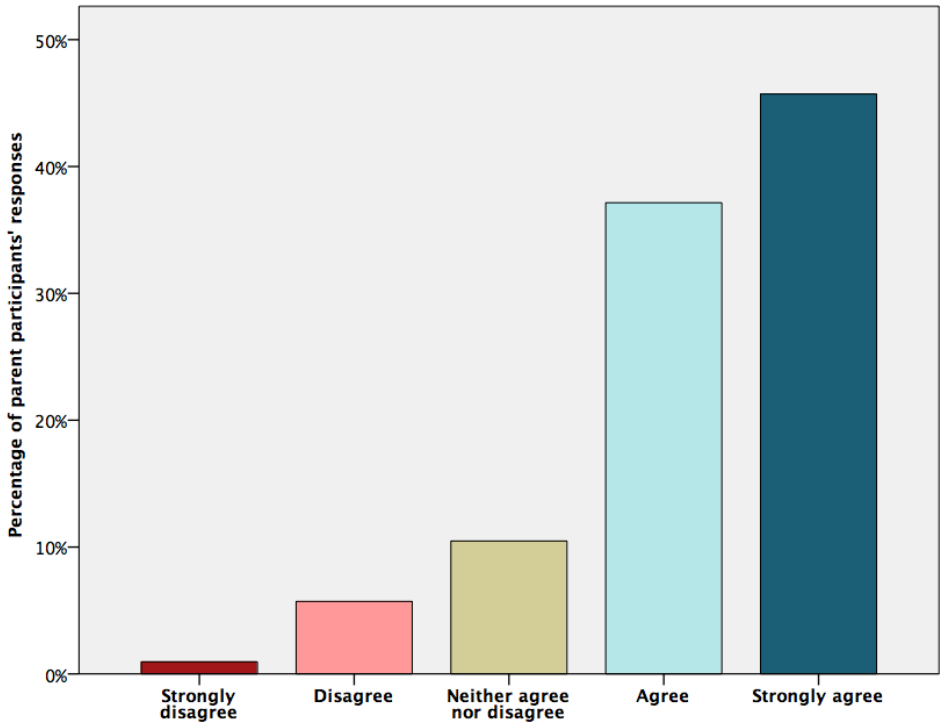

Figure 21: Parent participants' response to the question "I am concerned about my child's safety when they are online"

4.6.2 Parents' concerns about their child's password practices and the threats to which the child is exposed

Most parent participants were concerned about their child's safety when he/she is online (Figure 21). As shown in Figure 22, they are mostly concerned about their child talking to a stranger (86%), being exposed to explicit content (85%) and sharing personal information with strangers(84%).

Most participants either created an account *with* their child (53%) or created an account *for* the child (30%). As shown in Figure 23, 72% of the parent participants reported that they follow the recommended minimum age requirements for creating accounts on online websites or applications for their child. Parent participants (56%) also reported that they do not share their own password with their child, but they believe (58%) that the child has figured out one or more of their passwords.

Parent participants reported various strategies they use to teach their child to

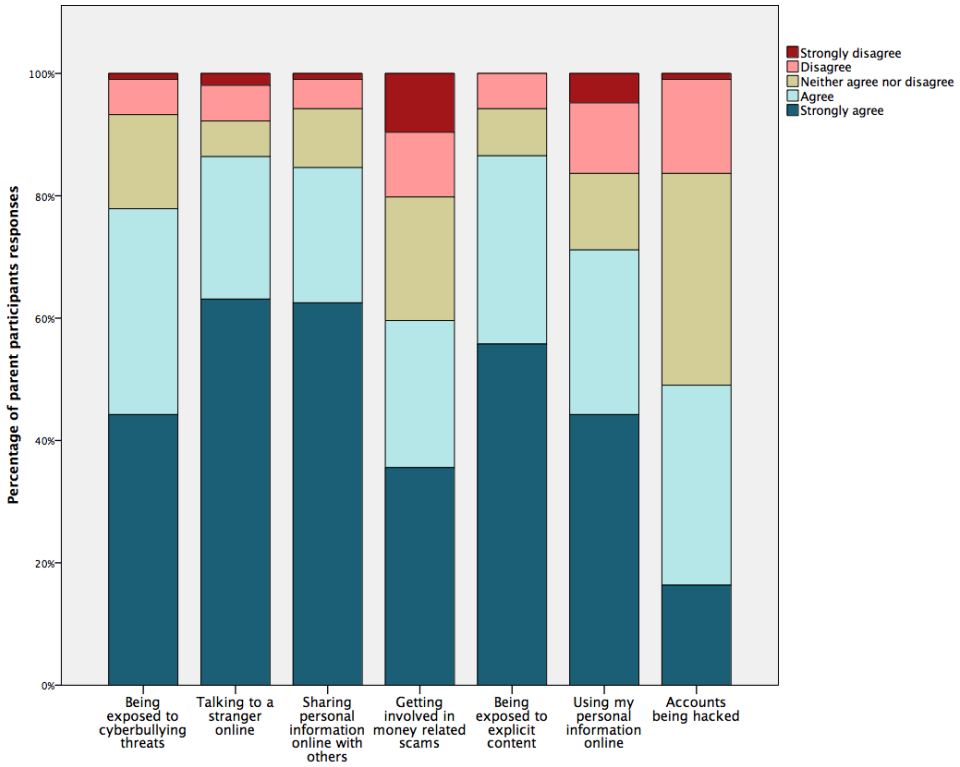

Figure 22: Parent participants' concerns when their child is online

create secure passwords (Figure 24). Most participants reported that they teach their children to create different passwords on different websites (71%) and not to use the parent participants' or their personal information as part of passwords (76%). Some (41%) parent participants reported that they teach their child to create simple passwords that are easy to remember.

Parent participants were asked what strategies they used to help their child manage their passwords. As shown in Figure 25, almost half of the parent participants (49%) reported that they teach their child not to share their password with friends or strangers, and only 10% of the participants teach their children not to write down their passwords.

Parent participants were asked if their child often forgets their password. As shown in Figure 26, fewer than half of the parent participants reported that their child forgets his/her passwords. Only 13% of the parent participants reported that they reset the password for the child when he/she forgets it, and 42% of them reported that their child resets the password themselves. It could also be that someone other

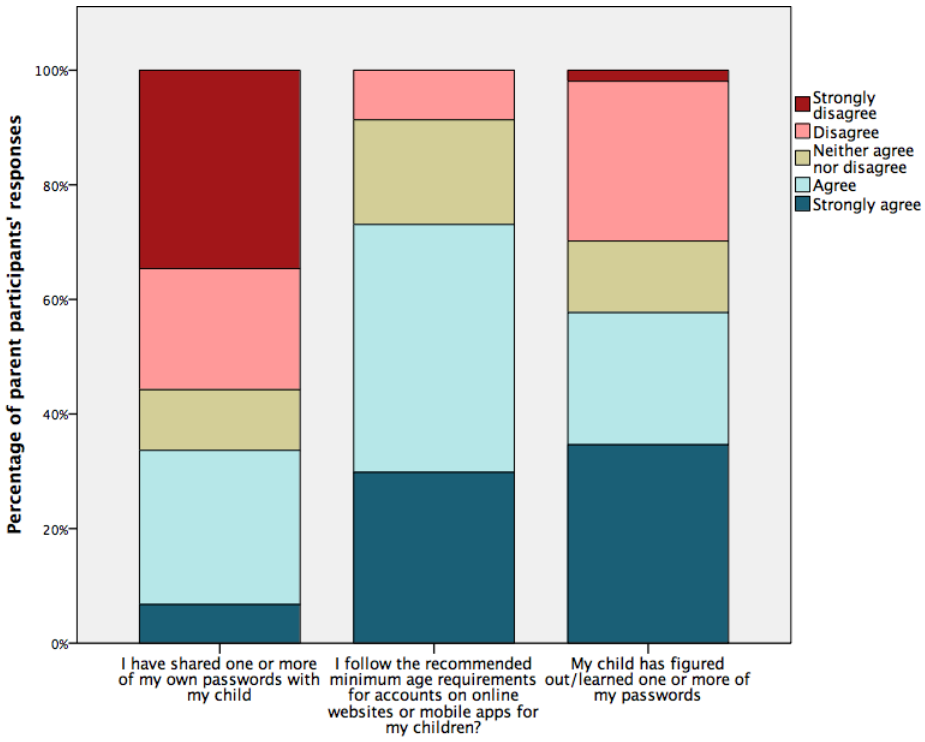

Figure 23: Parent participants' response to the questions related to their password behaviors

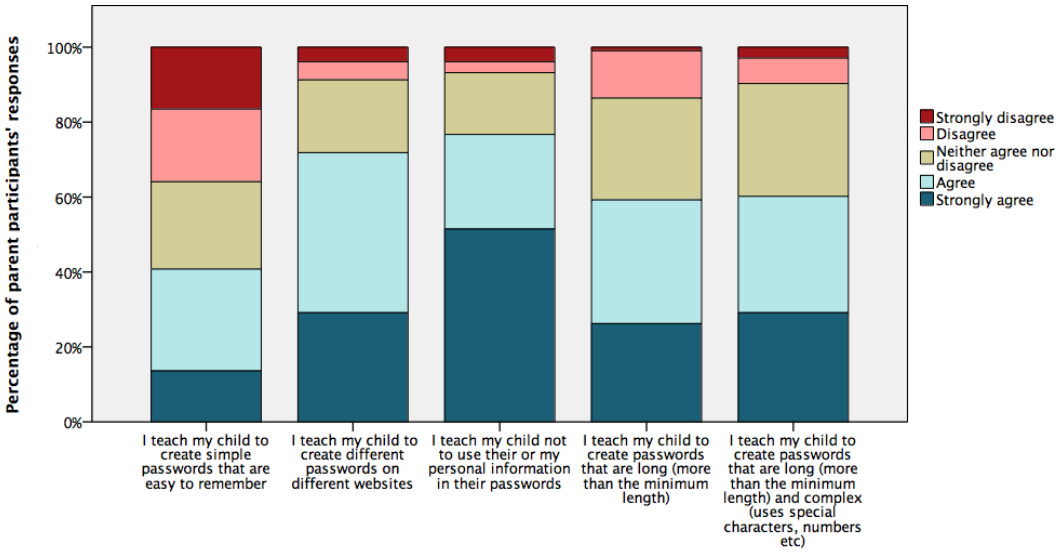

Figure 24: Different techniques parent participants teach their child about creating secure passwords

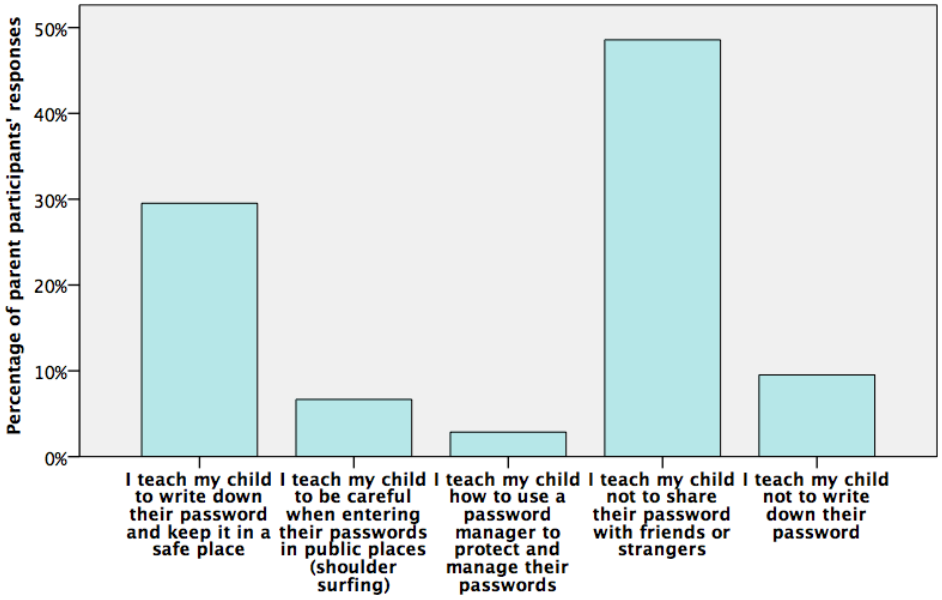

Figure 25: Strategies participants used to help children manage their passwords

than the child or the parent participants helps the child resets their password, such as teachers, siblings, relatives.

As shown in Figure 27, more than half (59%) of parent participants reported that their child tries to remember their password without writing it down or storing on their phone. However, some reported that their child writes down their passwords (30%) and uses simple passwords (39%) to make it easier to remember them.

4.6.3 Parents' beliefs and practices about creating passwords and practicing safe online behaviors

As shown in Figure 28, more than half (64%) of parent participants think that their child creates secure passwords. However, only 40% believe that their child is safe online and 90% of them reported that they monitor their child's online activity.

As shown in Figure 30, most parent participants (80%) reported that they often talk to their child about online threats. They also reported (78%) that their child is only allowed to use websites and mobile apps after they have looked at it themselves. 55% of the parent participants (Figure 29) believe that parents/guardian/family members and the school should teach children about password creation and management

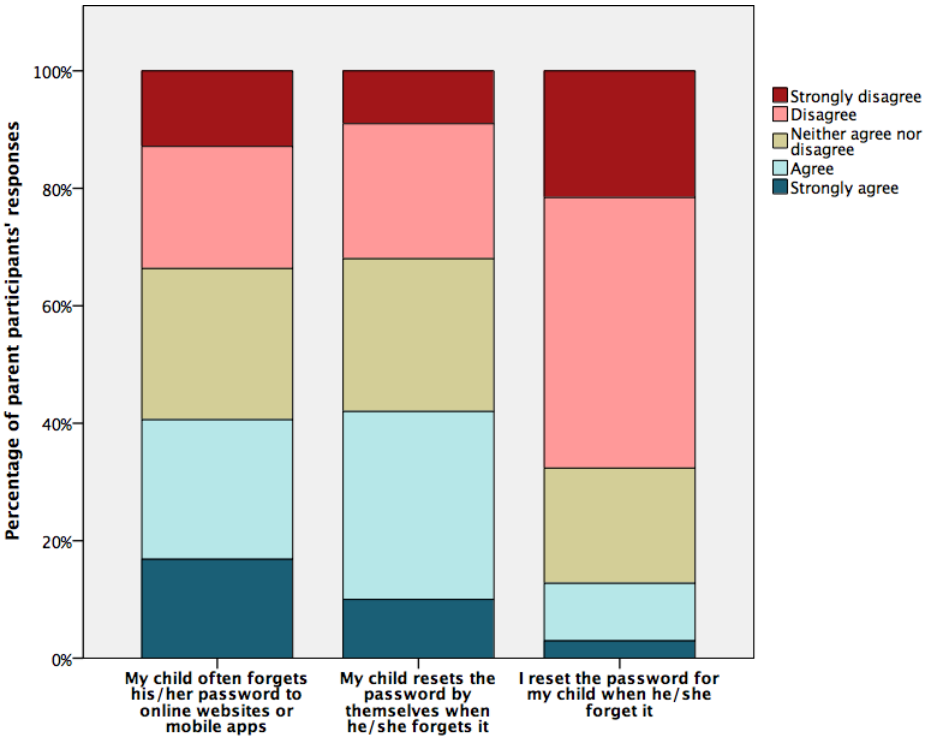

Figure 26: Strategies children use when they forget their passwords

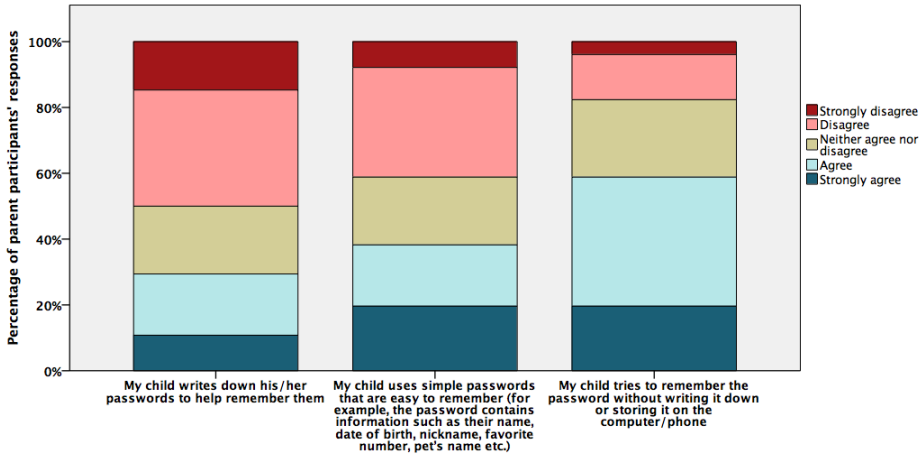

Figure 27: Strategies children use to help them remember their passwords

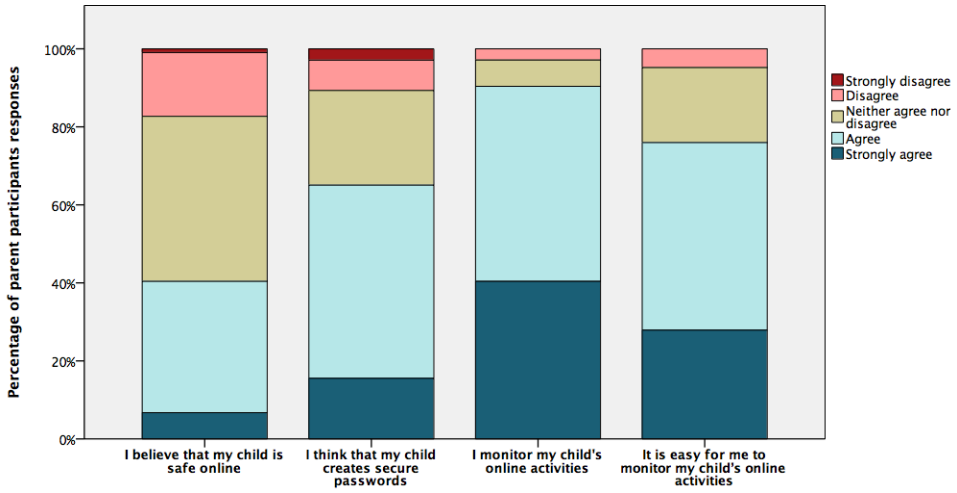

Figure 28: Parent participants' response to the questions related to their child's online safety

rules.

Parent participants (N=80) with more than one child were asked if their child shares his/her accounts with their siblings. As shown in Figure 30, fewer than half (43%) of the participants reported that their child shares his/her account with their siblings and 36% reported that their child always reuses the same password on multiple accounts.

Parent participants were asked what they thought about rules/policies around children's accounts. They reported that on average the minimum password length for children's account should be 8 characters. Parent participants also believed that children could create their passwords and understand different password rules at age 11. As shown in Figure 31, most parent participants (70%) reported that children's websites or mobile apps should require an account to login and that parental controls should be added to the child's devices.

Parent participants were asked what the biggest risk to their child's account is. We grouped participants' free-form responses into 7 categories (listed below). Some parent participants responded with more than one risk. Each of their risks was included in the appropriate category. For example, one parent participants' response was "Giving out personal information or social hacking.". Their response was categorized into two categories: "Being hacked" and "Sharing personal information online

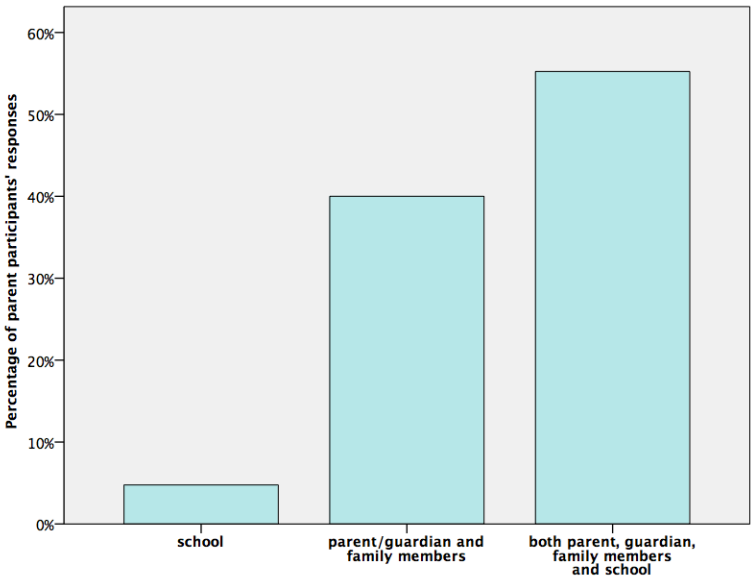

Figure 29: Participants' response to the question "Who should teach children about password creation and management rules?"

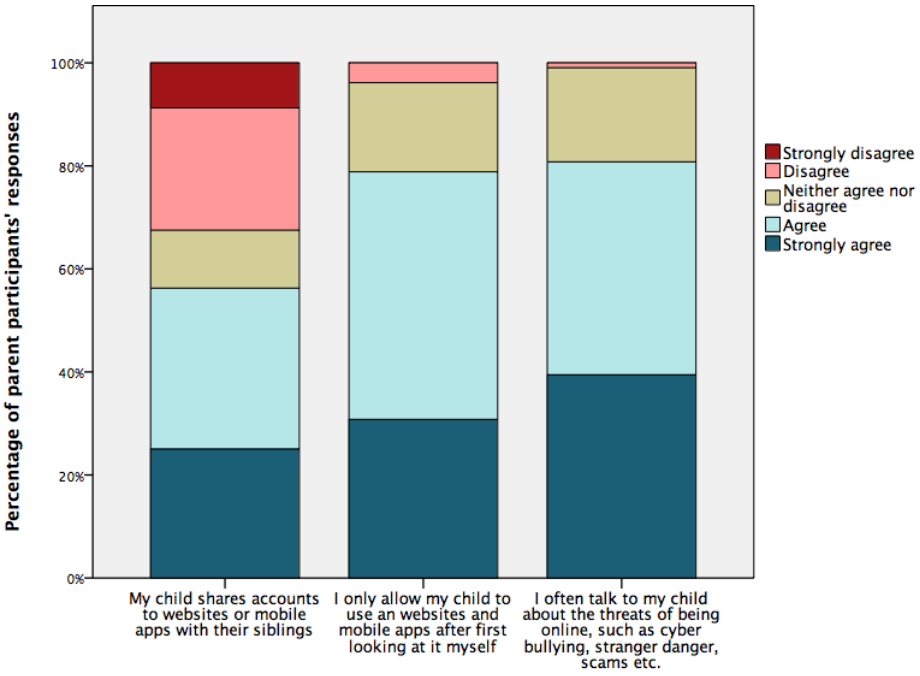

Figure 30: Parent participants' response to the questions related to their child's password behaviors

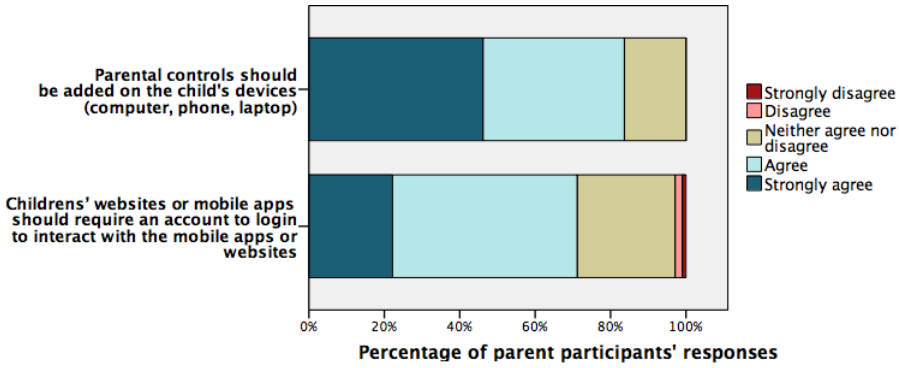

Figure 31: Parent participants' beliefs about children's accounts

with others". Appendix J has a complete list of parent participants' responses.

1. Being exposed to cyberbullying threats (N=8)
2. Talking to a stranger online (stranger danger) (N=9)
3. Sharing personal information online with others (N=9)
4. Getting involved in money related scams (N=3)
5. Being exposed to explicit/inappropriate content (N=5)
6. Being hacked (N=41)
7. Other (safety, security, identity theft, abuse, etc.) (N=7)

Based on the above categories, 36% of the parent participants reported the biggest risk to their child account is being hacked, consequently their personal information would get exposed to threats. 10% of the parent participants reported that it was sharing personal information online with others (Figure 32).

Parent participants (30%) reported they or someone they knew had experienced a security attack. From these parent participants, the ones who provided more information about the incident reported that they or someone they knew were hacked. Parent participants (13%) also reported that a particular incident had influenced their behavior towards online security and safety. These incidents included being hacked, someone taking over the parent participants' computer, a Trojan attack,

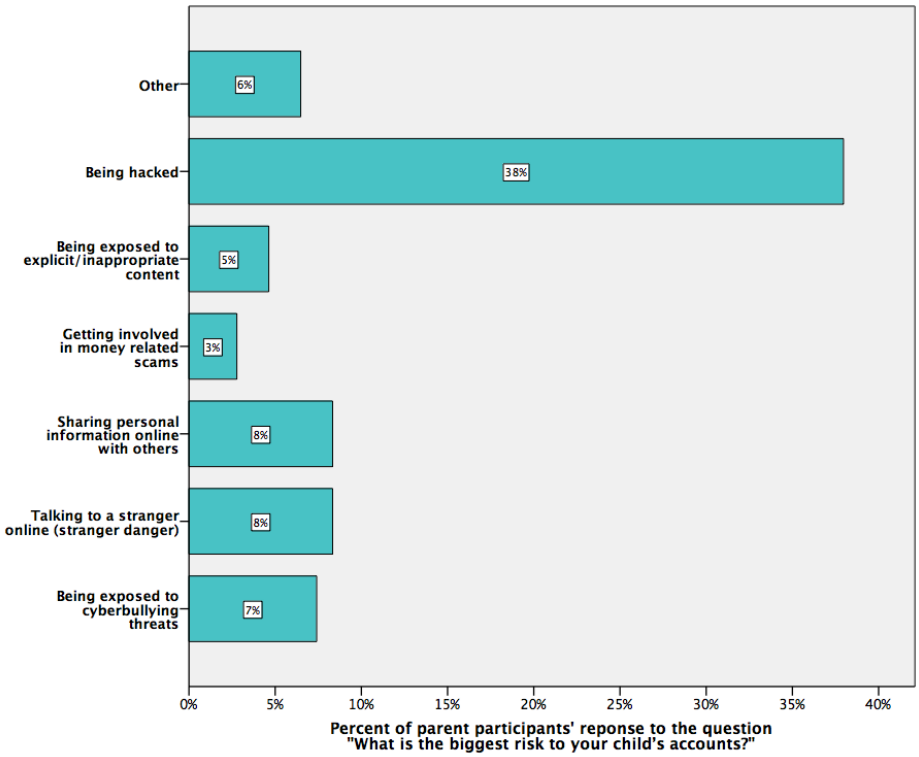

Figure 32: Participants' response to the question "What is the biggest risk to your child's accounts?"

having credit card information stolen, spending money and purchases that participants did not make. For example, one parent participant reported the incident as "being hacked, I am more careful when I receive emails from unknown sources".

Summary

From the above results, it seems like participants are somewhat aware of security cues, create secure passwords, and they are concerned about their child's safety when he/she is online and monitor their activities. Participants are concerned about stranger danger, exposure to explicit content, sharing personal information, cyberbullying, money related scams and child's accounts being hacked. Participants teach their children various techniques to create secure passwords, and they use various strategies to help them manage and remember their passwords. Participants also believe that their child creates secure passwords, shares their passwords with siblings and that parental controls should be added to children's accounts.

4.6.4 Composite variables

We created five composite variables (listed below) to understand the interaction between the parent participants' level of concern, belief in their child's password practices, teaching their child to create secure passwords, their level of proactive awareness, and their password creation practices. As well, we hoped to understand if the variables are affected by the child's age, child's gender, parent participants' age, gender or their education. We grouped survey questions related to the variable to generate the variable score. Some of the survey questions were not related any of the variables, and these were not included. A complete list of questions for each variable is shown in Appendix K.

Each variable consisted of an approximately six questions that were obviously addressing related subjects. These questions were in a Likert scale format. We reviewed each question to ensure that it was aligned in the same direction and was answering a similar question. A parent participants' score for a variable was calculated by taking an average of their responses to questions related to the variable.

concern Parent participants' level of concern about their child's safety when he/she is online (a higher score represents that a parent participant is more concerned about their child's safety). The variable was computed from 7 questions of the survey.

belief Parent participants' belief that their child creates secure passwords (a higher score represents that a parent participant believes that their child creates secure passwords). The variable was computed from 5 questions of the survey.

teaching Parent participants' efforts at teaching their child to create secure passwords (a higher score represents a parent participant teaching their child to create secure passwords). The variable was computed from 5 questions of the survey.

proactive awareness Participants' level of proactive awareness of security-related contextual cues (a higher score represents a parent participant who is more

Table 5: Description of correlation strength for different values of ρ

$\rho = 1$ or ρ= -1	strongest positive or negative linear relationship
0 <ρ <(+/-).19	very weak (positive or negative)
(+/-).20 <ρ <(+/-).39	weak (positive or negative)
(+/-).40 <ρ <(+/-).59	moderate (positive or negative)
(+/-).60 <ρ <(+/-).79	strong (positive or negative)
(+/-).80 <ρ <(+/-)1	very strong (positive or negative)

aware of security-related contextual cues, such as checking links before clicking them). The variable was computed from 5 questions of the survey.

password creation A parent participants' efforts at creating passwords that follow security guidelines (a higher score represents a parent participant creating more secure passwords). The variable was computed from 6 questions of the survey.

Interaction between the variables

We were interested in finding the relationship between the five composite variables defined above: concern, belief, teach, proactive awareness and password creation. To understand this, Spearman correlation was used. Spearman correlation measures the strength and direction of a monotonic relationship between two variables. We used Spearman correlation because the five composite variables are ranked, ordinal and monotonically related. The Spearman correlation coefficient, ρ , ranges from +1 to -1. A value of ρ equal to +1 indicates a strong positive correlation between two variables and a value of ρ equal to -1 indicates a strong negative correlation. Table 5 lists out interpretation of correlation strength for different ρ values [13].

As shown in Table 6, there is a weak positive correlation between the concern and teaching variables (Figure 33[2]). This suggests that concerned parent participants are more likely to teach their child to create secure passwords. There is a weak negative correlation between the proactive awareness and belief variables (Figure 34), suggesting that parent participants who are aware of security-related cues are unlikely to believe that their child creates secure passwords.

[2]We used box plots to illustrate our data rather than the more conventional scatter plots because scatter plots are ineffective at representing ordinal data.

There is a moderate positive correlation between the proactive awareness and teaching variables (Figure 35), suggesting that parent participants who are proactively aware of security-related threats are more likely to teach their child to create secure passwords.

There is a moderate positive correlation between the password creation and proactive awareness variables (Figure 36), suggesting that parent participants who are aware of security-related cues are more likely to create secure passwords.

There is a moderate positive correlation between the password creation and teaching variables (Figure 37), suggesting that parent participants who create secure passwords are more likely to teach their child to create secure passwords.

Table 6: Results of correlation among the five variables

	concern	**belief**	**teaching**	**proactive awareness**	**password creation**
concern	-	ρ (105)=.18, p=.06	ρ (103)=.28, p<.01,	ρ (104)=.03, p=.79	ρ (104)=.16, p=.10
belief	-	-	ρ (103)=-.12, p=.23	ρ (104)=-.35, p<.01	ρ (104)=-.11, p=.25
teaching	-	-	-	ρ (102)=.39, p<.01	ρ (102)=.50, p<.01
proactive awareness	-	-	-	-	ρ (103)=.45, p<.01
password creation	-	-	-	-	-

Participants who create secure passwords are more likely to teach their child to do the same. This may be the reason they believe that their child creates secure passwords. However, parents who are concerned about their child's safety when he/she is online are less likely to believe that their child is creating secure passwords. This may be the reason they teach their child to create secure passwords.

Effect of child's age, gender, parent participants' age, gender and education on the variables

We were interested in finding if a child's age, gender, parent participants' age, gender, and education affect the five composite variables: concern, belief, teach, proactive awareness and password creation. To understand this, we performed two tests; Mann-Whitney and Kruskal-Wallis. The Mann-Whitney U test is non-parametric test used to test if there a difference between two categories of an independent variable and the

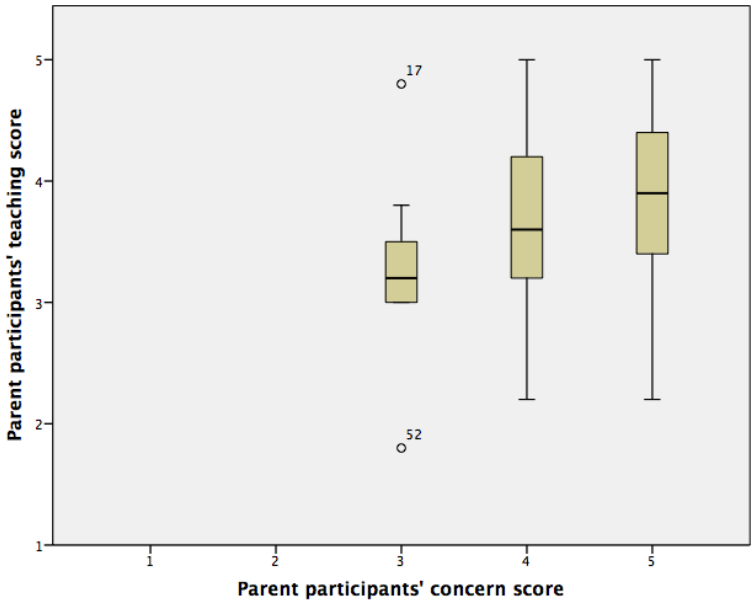

Figure 33: Box plot of parent participants' concern score and teaching scores

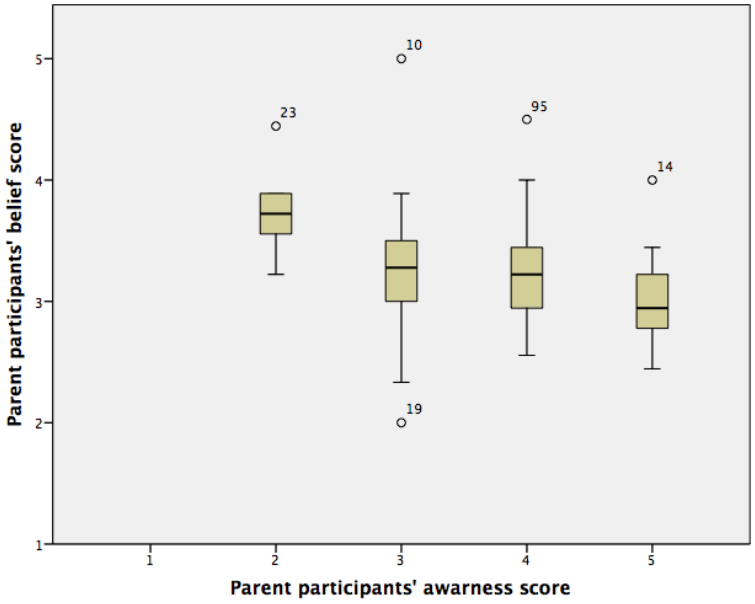

Figure 34: Box plot of parent participants' awareness and belief scores

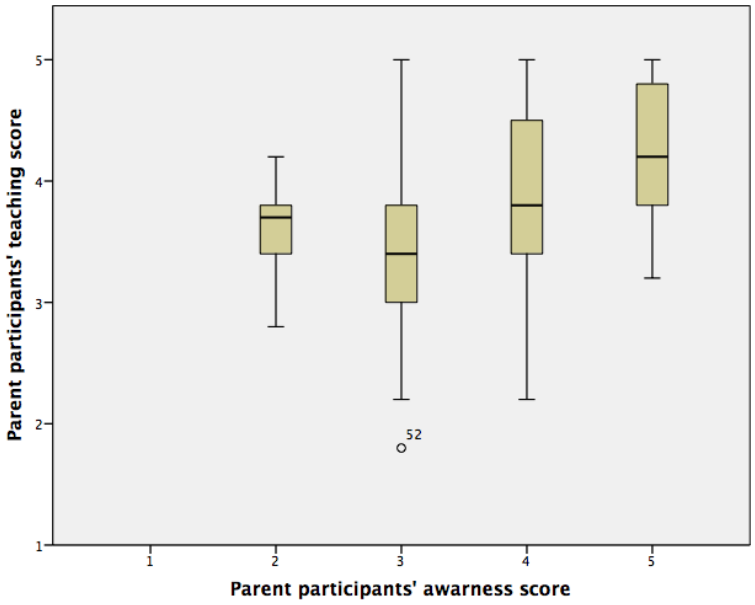

Figure 35: Box plot of parent participants' awareness and teaching scores

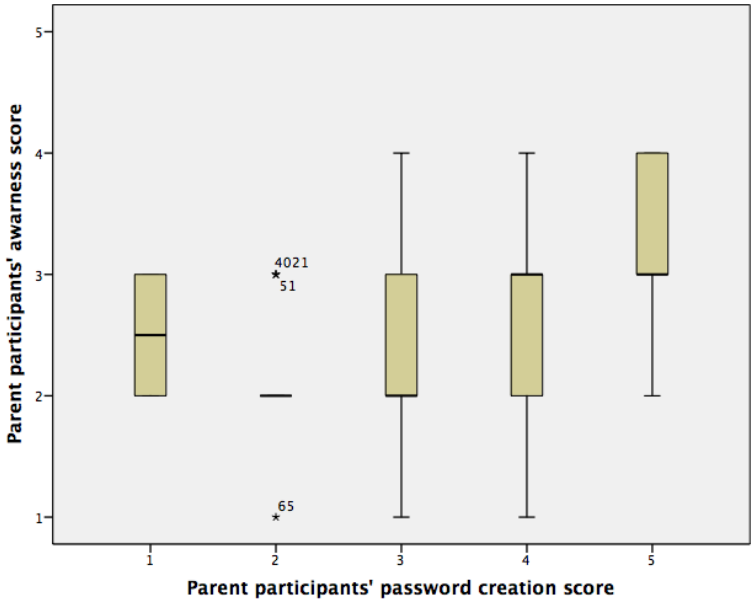

Figure 36: Box plot of parent participants password creation and awareness scores

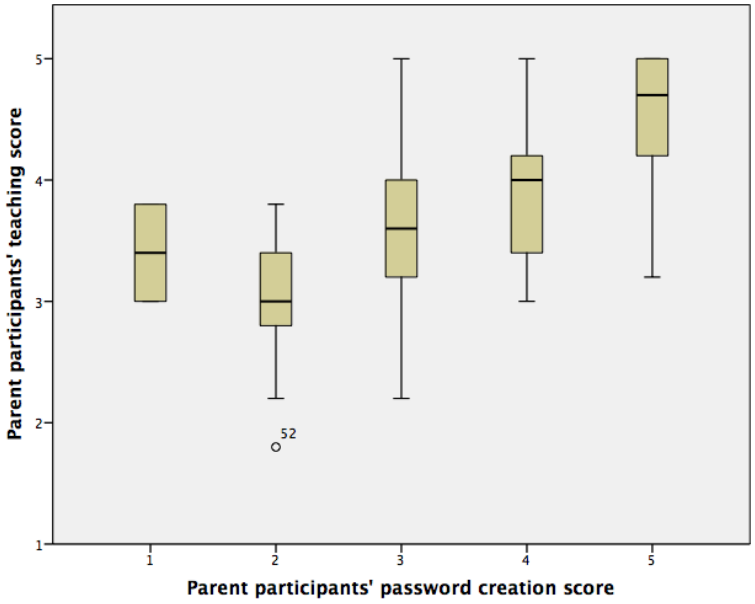

Figure 37: Box plot of parent participants' password creation and teaching scores

Table 7: Results of Mann-Whitney tests on parent participants' gender and children's gender and the five composite variables

	concern	**belief**	**teaching**	**proactive awareness**	**password creating**
Parent participants' gender	U=1220 p=0.83	U=1181 p=0.65	U=1054 p=0.36	U=789 p<.01	U=1124 p=0.49
Children's gender	U=1302 p=0.76	U=1281 p=0.69	U=1138 p=0.28	U=1252 p=0.63	U=1173 p=0.30

dependent variable. The dependent variable needs to be measured on an ordinal or continuous scale.

We used a Mann-Whitney U test to understand a difference in the five composite variables and the children's or parent participants' gender. The data for five composite variables are not normally distributed, and are measured on an ordinal scale. In our test, the independent variables are children's and parent participants' gender. The dependent variables are concern, belief, teaching, proactive awareness, password creation. Table 7 shows the results Mann-Whitney U tests at the .05 significance level. The results of Mann-Whitney U test show that the five composite variables did not significantly differ for children's or parent participants' gender. However, participants' gender significantly affected participants' level of awareness, where fathers were more aware than mothers.

Kruskal-Wallis is a rank based non-parametric test. It is used to test if there is a statistically significant difference between more than two categories of an independent variable and the dependent variable. The dependent variable needs to be measured on an ordinal or continuous scale. We used Kruskal-Wallis tests to understand the difference in five composite variables and children's age, participants' age and education. In our test, the independent variables are children's age, parent participants' age, and education. The dependent variables are concern, belief, teaching, proactive awareness, password creation.

Parent participants' age ranged from 21 to 60 years old. They were grouped into five age groups 21-31, 32-36, 37-40, 41-47 and 48-60 year olds. The parent participants were grouped to have approximately the same number of participants in each age group. Children's age ranged from 6 to 13 year old. We grouped them into four age groups, 6-7, 8-9, 10-11 and 12-13 year olds. As shown in Table 8, participants' education, age and children's age did not affect any of the five composite variables.

Table 8: Results of Kruskal-Wallis test on participants' age, education, child's age and the five variables

	Participants' level of concern	**Participants' belief of their child's password practices**	**Participants teaching secure passwords practices**	**Participants' level of awareness**	**Participants' password creating practices**
Participants' age	$\chi^2(4)=3.61$, p=0.46	$\chi^2(4)=8.70$, p=0.07	$\chi^2(4)=2.37$, p=0.67	$\chi^2(4)=5.86$, p=0.21	$\chi^2(4)=2.92$, p=0.57
Participants' education	$\chi^2(4)=1.74$, p=0.78	$\chi^2(4)=4.78$, p=0.31	$\chi^2(4)=1.91$, p=0.75	$\chi^2(4)=4.69$, p=0.32	$\chi^2(4)=7.48$, p=0.11
Child's age	$\chi^2(3)=1.32$, p=0.73	$\chi^2(3)=4.69$, p=0.20	$\chi^2(3)=1.10$, p=0.77	-	-

4.7 Discussion

Parent participants completed a survey related to parents' password practices, their children's password practices and what they teach their children about creating secure passwords and staying safe online.

The findings of the study were: concerned parents are more likely to teach their child to create secure passwords, parents who are aware of security-related cues are

more likely to create secure passwords; believe that their child does not create secure passwords, and teach them to create secure passwords. Each of the findings is discussed below in detail.

4.7.1 Parent participants' level of concern and teaching their child to create secure passwords

Parent participants are concerned about their children's safety when they are online regardless of their age. They are heavily involved in creating and managing their child's passwords. Parent participants monitor their children's online activity, talk to them about online threats, teach them strategies to protect their password and teach them to create secure passwords.

The result of our study showed that parent parents are teaching children strategies to create secure passwords. The most common strategies were: not to use personal information in the passwords and to create different passwords on different websites. 40% of the parent participants reported that they teach their children to create simple passwords that are easy to remember. We are not aware of what these simple passwords contain. It may be that these passwords are simple for a child to remember and they are secure. 30% of parent participants reported that their children use simple passwords that are easy for them to remember. They reported that these simple passwords contained children's name, date of birth, nickname, favorite number, etc., therefore making them weak and vulnerable to threats.

We believe that children learned this method of creating passwords from their parents. Hundlani et al. [17] reported that parents used weak password management strategies as a result of having to reset their child's password. These strategies included using a weak or no password, writing the password down in a visible location and reusing passwords across accounts. Similar findings were reported by Zhang-Kennedy et al. [40] who found that the burden of remembering children's password fell on adults. Children often forgot their password and therefore were encouraged by adults to create simple dictionary passwords that are easy for them to remember. These strategies make it easier for parents to manage their children's password but

they also make the children's passwords vulnerable to threats. We need to understand better how to teach children to create secure passwords that are easy for them to remember so that they do not forget them. This would too reduce the burden on parents to manage their child's password.

Parent participants used different strategies to help children manage their passwords. Fewer than half of the parent participants taught their child not to share their passwords with friends or stranger, and 30% taught them to write down their password and keep it in a safe place. Parent participants found it more important to teach their child not to share the password with friends or stranger than teaching them to use a password manager, writing down the password or keeping it in a safe place, indicating that parent participants have some understanding of strategies to manage the password in a secure manner.

We found that parent participants' education did not have an effect on their level of awareness of security-related cues and them creating secure passwords. We thought that more educated parents would be more aware of security-related cues and therefore create secure passwords. However, our results did not show this; education did not have an effect on parent participants' level of concern, awareness of security-related cues or them creating secure passwords. Another factor such as how well parent participants are informed about technology could have affected their level of awareness and them creating secure passwords.

4.7.2 Parent participants' level of awareness and teaching their child to create secure passwords

Most parent participants are aware of security-related cues and create secure passwords. Based on the results, parent participants have a basic understanding of characteristics of a strong password (non-dictionary word, special character, number, length, mixed character case). They rated the password "camila" as least secure and "Hmjt05!" as highly secure. They also rated the password "987654321" as being more secure than the password "camila". We believe that parent participants who have a good understanding of what makes a password strong are more likely to create secure passwords.

We found that parent participants who are aware of security-related cues are less likely to believe that their child creates secure passwords and therefore teach their child to create secure passwords. Based on the findings, we believe that to teach children to create secure passwords; parent participants need to aware of security-related cues, understand what makes a password strong and create secure passwords themselves. By creating secure passwords themselves, parent participants would have a better understanding of what makes a password harder/easier to remember. Overall, we need to look at strategies to help parents be more aware of security-related threats.

4.7.3 Conclusion

Our key finding is that parents who are more aware of security-related cues are more likely to create secure passwords, believe that their child does not create secure passwords and teach their child to create secure passwords. As mentioned earlier, most parent participants help their child create his or her account and manage their passwords. Therefore, it is important for parents to have a good understanding of creating secure passwords. This will allow them to teach their child to create secure passwords. The findings about parents' awareness of security related cues also suggest that a more holistic knowledge on security also helps them teach their children to protect themselves from threats.

Limitations

The study had several limitations, relating to the questions used in each of the composite variables and parent participants responding in a socially acceptable manner. Each composite variable had only a few questions. Therefore, we need to be careful in interpreting the findings. To get a better understanding of the variables, we should include more in-depth questions relating to the variable. We could also conduct a lab study with a parent and child pair where the parent to helps/teaches the child to create a secure password. This would allow us to understand what parents teach their children about secure passwords instead of relying on self-reports.

In the survey, parent participants were presented with options for most of the

questions. Parent participants may not want to be perceived as "bad" parents, therefore, they could have responded to questions in a more socially acceptable manner. A correlation was found between a few composite variables (proactive awareness and teaching). These relationships need to be further tested in a lab setting to understand them better. Also, we need to conduct further studies to test the reliability and validity of each composite variable to ensure that it measures what it intends to. Despite these limitations, our study does provide insight into what parents teach their children on creating secure passwords and how proactively aware parents teach their child to create secure passwords.

Chapter 5

Conclusions

In our research, we were interested in understanding the type of passwords children create with different password rules, and how they create these passwords. We were also interested in understanding parents' password behaviors and what they teach their children about creating secure passwords. The following sections highlight findings from the two studies, their limitations, our contributions and future work.

5.1 Study 1: Findings

We conducted a study with children ages 11 to 13 years old. Children were asked to create passwords on three websites with different passwords rules. At the end of the study, children were asked to recall the passwords they created in the study. The results of the study suggested that children had a basic understanding of protecting their personal information. They did not want a stranger to get access to their emails or messages because they were considered private. However, children did not have a good understanding of how to protect their personal information and with whom to share it. Most children were comfortable with their parents having access to their accounts but not their siblings or friends. Children were afraid that siblings and friends would 'mess up' their accounts — not because they would have access to their personal information.

It also seemed like children did not seem to know what makes a password weak or strong. Children created easy to remember passwords using their personal information and dictionary words. They believed that these passwords would be hard for a stranger to guess. However, they might not realize that this method of creating passwords puts them at risk. We thought that children learned this way of creating passwords from their parents/guardian. To understand this, we conducted a second study with parents.

5.2 Study 2: Findings

We surveyed parents to understand their password behaviors and the strategies they teach their children about creating secure passwords. The results of the study suggested that parents created somewhat secure passwords, and they were somewhat aware of security-related cues. We believe that to teach children to create secure passwords, parents themselves need to know about creating secure passwords. Parents in our study had a basic understanding of characteristics of a strong or a weak password; they rated a password with random characters as highly secure and a password with a user's name as least secure. We found that parents who were more proactively aware of security-related cues were more likely to create secure passwords themselves and teach their children to create secure passwords.

Similar to what was shown in existing research [17, 40], parents in our study were involved in creating children's accounts and resetting their passwords. As well, parents were also concerned about their children's safety when they were online. Parents' biggest concern was their children's account being hacked. We are not sure if they are aware of other threats that are as harmful as being hacked, such as children sharing their personal information with others online. Parents reported that they often talk to children about different types of threats and teach them strategies to protect their passwords. However, some parents reported that they taught their children to create simple passwords and that their children create passwords using their personal information and dictionary words. Research has shown that parents teach their children to create simple passwords to avoid having to manage their children's passwords and to make it easier for children to remember their passwords [40]. Therefore, children are learning from their parents to create weak passwords. We are concerned that children will carry this behavior of creating passwords into adulthood. Therefore, it is imperative for children to learn at a young age why it is important to create secure passwords, how to create secure passwords and strategies to help them remember the passwords.

5.3 Limitations

Both studies had limitations. In our first study we found that children had no difficulty in creating passwords and remembering them for a short period. However, they might not remember them for a long period. We did not test the children's passwords for long-term memorability. The two main limitations of our second study were the reliability and validity of the survey and the five composite variables. The five composite variables were used to measure parents' level of awareness, their concern, their password behaviors and their efforts at teaching children to create secure passwords. Parents might have responded in a socially acceptable manner to the questions related to their password behaviors and the strategies they teach their children to create secure passwords. Parents might not behave the same way in their real life as they reported in the survey. A subset of questions were used to compute scores for the composite variables. On average, each variable had six questions. We believe that more questions that reflect the variables can be included in computing variables' scores. Another limitation of our studies was that the children from the first study and the parents from the second study were from a different sample set and recruited through different methods, which could have introduced unexpected bias and affected in any comparisons made. The differences we observed between children and adults could also partially stem from having recruited from different populations. This could be addressed by conducting a study with parent and child pairs.

5.4 Contributions

Despite the limitations, our research provided insights on the type of passwords children create and the parents' behavior that would make them more likely to teach the children to create secure passwords. As part of our research, we conducted two studies, one with the children and another with the parents. From the first study, we found that children create simple passwords that are easier for them to remember; they *believe* that they create secure passwords and children do not find it challenging to create passwords with different password rules except one (the special character rule). Therefore, we recommend that systems designed for children could include

password rules such as mixed character case, numbers, special characters (but that needs to be first explained to the children). Based on our results, we also recommend careful language relating to password policies (e.g "symbols" may be more meaningful to children than "special characters").

From our second study, we found that parents are concerned about their children's safety but use weak password management strategies for their children's accounts. To alleviate the burden on parents, children need to learn strategies to create secure passwords and how to remember them. We also found that parents who are highly aware of security cues are more likely to create secure password themselves and teach their children to do the same. Therefore, to increase the children's chances of learning to create secure passwords parents need to have a better understanding of creating secure passwords and have a comprehensive security knowledge to help protect themselves from various threats. Our results were largely as we had expected. However, given how little research exists in this important area, our results offer empirical evidence contributing to a foundation in the area.

5.5 Future work

Further studies need to be conducted to address the limitations of the first and second studies. In the first study, short-term memorability tests showed positive results; children remembered their highly complex password for the duration of the study. We need to conduct further studies to understand the type of passwords rules that are easier for children to remember. In the second study, parents responded to a survey. We need to understand whether parents' responses are similar to their real behaviors. We could conduct lab sessions with parents and children to understand parents' password behaviors and the strategies they teach their children to create secure passwords. As well, further studies need to be conducted to test for reliability and validity of the five composite variables. We used the SeBIS scale [11, 12] scale to measure parents' level of awareness. Further research needs to be conducted to find other scales that complement the SeBIS awareness sub-scale.

Children process information differently than adults. We need to develop training material targeted for children to help them understand the importance of creating

secure passwords. We also need to teach children strategies to create secure passwords and help them remember their passwords. Parents need to learn about security practices that help to protect them from threats; which will help them teach their children to do the same.

Bibliography

[1] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. In *2008 Second Asia International Conference on Modelling; Simulation (AMS)*, pages 396–403, May 2008.

[2] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[3] Hala Assal, Ahsan Imran, and Sonia Chiasson. An exploration of graphical password authentication for children. *CoRR*, abs/1610.09743, 2016.

[4] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, pages 553–567, Washington, DC, USA, 2012. IEEE Computer Society.

[5] WE Burr, DF Dodson, and WT Polk. Information security: Electronic authentication guideline nist. Technical report, Tech. Rep. Special Rep. 800-63, 2006.

[6] Jasmina Byrne, Daniel Kardefelt-Winther, Sonia Livingstone, and Mariya Stoilova. Global kids online: research synthesis 2015-2016. 2016.

[7] Michelene T. H. Chi. Short-term memory limitations in children: Capacity or processing deficits? *Memory & Cognition*, 4(5):559–572, Sep 1976.

[8] Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa, Bruna Freitas Machado, Alain Forget, Nicholas Wright, Gerry Chan, and Robert Biddle. The mvp web-based authentication framework - (short paper). In *Financial Cryptography*, pages 16–24, 2012.

[9] Jasper Cole, Greg Walsh, and Zach Pease. Click to enter: Comparing graphical and textual passwords for children. In *Proceedings of the 2017 Conference on Interaction Design and Children*, IDC '17, pages 472–477, New York, NY, USA, 2017. ACM.

[10] Margaret Anne Defeyter, Riccardo Russo, and Pamela Louise McPartlin. The picture superiority effect in recognition memory: A developmental study using the response signal procedure. *Cognitive Development*, 24(3):265 – 273, 2009.

[11] Serge Egelman, Marian Harbach, and Eyal Peer. Behavior ever follows intention? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: CHI'16*, pages 1–5, 2016.

[12] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2873–2882, New York, NY, USA, 2015. ACM.

[13] J.D. Evans. *Straightforward Statistics for the Behavioral Science*. Psychology Series. Brooks/Cole, 1995.

[14] Simson Garfinkel and Heather Richter Lipford. *Usable Security:History, Themes, and Challenges*. Morgan & Claypool, 2014.

[15] Paul A Grassi, Michael E Garcia, and James L Fenton. Digital identity guidelines. *NIST Special Publication*, 800:63–3, 2017.

[16] Cormac Herley and Paul van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security and Privacy*, 10(1):28–36, January 2012.

[17] Kalpana Hundlani, Sonia Chiasson, and Larry Hamid. No passwords needed: The iterative design of a parent-child authentication mechanism. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '17, pages 45:1–45:11, New York, NY, USA, 2017. ACM.

[18] Dev Raj Lamichhane and Janet C. Read. Investigating children's passwords using a game-based survey. In *Proceedings of the 2017 Conference on Interaction Design and Children*, IDC '17, pages 617–622, New York, NY, USA, 2017. ACM.

[19] J. Richard Landis and Gary G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174, 1977.

[20] Effie Lai-Chong Law, Dawn E Watkins, Joanna PL Barwick, and Elee S Kirk. An experiential approach to the design and evaluation of a gamified research tool for law in children's lives. In *Proceedings of the 15th International Conference on Interaction Design and Children*, pages 322–333. ACM, 2016.

[21] Sonia Livingstone, John Carr, and Jasmina Byrne. *One in Three: Internet Governance and Children's Rights*. 2015.

[22] T. Mendori, M. Kubouchi, M. Okada, and A. Shimizu. Password input interface suitable for primary school children. In *International Conference on Computers in Education, 2002. Proceedings.*, pages 765–766 vol.1, Dec 2002.

[23] Donald A. Norman. Design rules based on analyses of human error. *Commun. ACM*, 26(4):254–258, April 1983.

[24] Allan Paivio, T. B. Rogers, and Padric C. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 11(4):137–138, Apr 1968.

[25] Janet C Read and Russell Beale. Under my pillow: designing security for children's special things. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pages 288–292. British Computer Society, 2009.

[26] Janet C. Read and Brendan Cassidy. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, IDC '12, pages 200–203, New York, NY, USA, 2012. ACM.

[27] M. Renaud and R. Mulji. Authentication system, such as an authentication system for children and teenagers, November 8 2007. US Patent App. 11/693,438.

[28] Jennifer A Rode. Digital parenting: designing children's safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pages 244–251. British Computer Society, 2009.

[29] M. A. Sasse. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. In *Proceedings of CHI2003 Workshop on Human-Computer Interaction and Security Systems*, 2003.

[30] Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2000.

[31] Claude E Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[32] Valerie Steeves. *Talking to Youth and Parents about Life Online*. 2012.

[33] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 15:1–15:14, New York, NY, USA, 2013. ACM.

[34] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 15:1–15:14, New York, NY, USA, 2013. ACM.

[35] Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255, Menlo Park, CA, 2014. USENIX Association.

[36] E. Tulving and Z. Pearlstone. Availability versus accessibility of information in memory for words. *Journal of Verbal Learning and Verbal Behavior*, 5:381–391–, 1966.

[37] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 1–12, New York, NY, USA, 2005. ACM.

[38] Nicholas Wright, Andrew S. Patrick, and Robert Biddle. Do you see your password?: Applying recognition to textual passwords. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 8:1–8:14, New York, NY, USA, 2012. ACM.

[39] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: empirical results. *IEEE Security Privacy*, 2(5):25–31, Sept 2004.

[40] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*, IDC '16, pages 388–399, New York, NY, USA, 2016. ACM.

Appendix A

Carleton UNIVERSITY
Canada's Capital University

Study 1: Parental Permission for Children Participation in Research

Title of research project: Evaluating user authentication for Children
Ethics Clearance number: 104813
Date of Ethics Clearance: July 13th, 2016
Ethics Clearance for the Collection of Data Expires: July 13th, 2018

Introduction

The purpose of this form is to provide you information that may affect your decision as to whether or not you want to participate in this research study. The person performing the research will describe the study to you and answer all your questions. Read the information below and ask any questions you might have before deciding whether or not to take part. If you decide to be involved in this study, this form will be used to record your permission.

To participate in the study, the child must be between 11 and 13 years old and a regular online user.

Purpose of the Study

If you agree, your child will be asked to participate in a research study to understand how children create password on websites. If you wish, you can stay with your child during the study, however they would complete the study on their own.

What is my child going to be asked to do?

If your child participates in this study, they will complete a pre-test interview, create an account on three prototypes of websites for designed for children and complete a

post-test interview. The participant would first be asked a few basic demographic questions. They would then be asked to complete a task on each of the three websites. To complete the task, the child would have to create an account with a password for each website. Passwords rules are different on each of three websites, therefore the password on each website would be different. The tasks on the website are simple and age-appropriate, such as completing a poll, quiz or playing a game. The creation of an account on the websites would help researchers understand the kinds of password children create. Finally, the participants would answer a few questions about their experience using the websites and creating the three different passwords. This is used to get feedback on the websites and to understand the strategies used to create a password, and to understand the participant's current understanding and use of passwords. This study will take approximately 45 minutes. There are no foreseeable risks to participating in this study. The child will not be asked to disclose any personally identifiable information. However if such information is voluntarily disclosed, it will be discarded from the analysis. The possible benefit of participation is to know more about your child's understanding of passwords.

Does my child have to participate?

No, your child's participation in this study is voluntary. Your child may decline to participate or to withdraw from participation at any time.

What if my child does not want to participate?

In addition to your permission, your child must agree to participate in the study. If you child does not want to participate they will not be included in the study and there will be no penalty. Even if your child initially agrees to be in the study, they can change their mind later without any penalty. Your child will receive a $15 gift card for Chapters and may keep the gift card even if they choose to withdraw.

How will your child's privacy and confidentiality be protected if s/he participates in this research study?

Your child's privacy and the confidentiality of his/her data will be protected by storing the data electronically on a password-protected computer. The consent forms will be stored separately from the digital transcribed text files in a locked file cabinet. Access will be restricted to those researchers directly involved with the research.

This research was funded through grant by Canadian Internet Registration Authority (CIRA).

This project was reviewed and received ethics clearance by the Carleton University Research Ethics Board – B (104813). Contact information for the CUREB-B Chair follows:

Dr. Shelley Brown, Chair, CUREB-B
613-520-ext. 1505
Shelley.Brown@carleton.ca
Carleton University Research Compliance Office
613-520-2600 ext. 4085
ethics@carleton.ca

The principal researchers involved in this research are:

Sumbal Maqsood,
Masters Student,
School of Computer Science,
Carleton University
1125 Colonel By Drive,
Ottawa, Ontario,
K1S 5B6
Tel:(613)709-7132,
Email: sumbalmaqsood
@cmail.carleton.ca

Sonia Chiasson,
Assistant Professor
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario
K1S 5B6
Tel:(613)520-2600 ext.1656,
Email:chiasson
@scs.carleton.ca

Robert Biddle,
Professor
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario
K1S 5B6
Tel:(613) 520-2600 ext. 6317,
Email: robert_biddle
@carleton.ca

Appendix B

Study 1: Verbal informed assent script for children

Hi, my name is Sumbal Maqsood, a student at Carleton University. I need your help to evaluate website designed for children.

First, you will need to answer a few questions about yourself. Then I will show three different websites, in which you will need to complete a simple task. Finally, you will need to answer a few questions about what you thought of the websites and the tasks you completed.

The information you tell me will be kept safely locked up. Nobody will know who said it except the people doing the research.

You do not have to join this study. It is up to you. You can say okay now and change your mind later. All you have to do is tell me that you want to stop. No one will be mad at you. Just let me know. You can also skip any question that you don't feel comfortable answering and still remain in the study.

To thank you for your help, I will give you a $15 gift card for Chapters. You can keep the gift card even if you decide to stop the interview.

Do you have any questions? Remember that you can ask questions at any time.

Do you want to try out the websites and answer some questions about them?

If yes, please say: yes, I will be in this research study If no, please say: no, I don't want to do this

Appendix C

Study 1: Pre-test questionnaire

The pre-test interview asks children some questions about them and about their usage of the Internet/technology/websites. All the communication would take place in English. The participants will be thanked at the end of the experimental session.

1. How old are you?
2. Gender
3. Which grade in school are you in?
4. Do you frequently download applications for the Internet?
    - Yes
    - No
5. Who creates an account for you on these websites/applications?
    - Myself
    - Parent/Guardian
6. Can you tell me which website/apps that you frequently use?
7. How often do you login into these websites?
    - Less than once a week
    - Once a week
    - Once a day
    - More than once a day
    - More than 10 times a day

Appendix D

Study 1: Questionnaire during the study

This interview would be conducted while participants are completing the study tasks and will be repeated for each website. It will ask children some questions about how they created passwords on the three websites.

1. What did you like about the website?
2. What did you dislike about the website? Why?
3. How did you create your password on this website ?
4. Did you find it easy to complete the task on the website?

Appendix E

Study 1: Post-test questionnaire

The post-test questionnaire asks children questions related to their experience of using the websites and the strategies they used to create passwords.

1. Did you find the easy to use the three websites and complete the tasks?
2. Which of the three website did you like the most? (images of the three sites shown to them)
   (a) Website A
   (b) Website B
   (c) Website C
   (d) Why ?
3. Which of the three website was your least favorite (images of the three sites shown to them)
   (a) Website A
   (b) Website B
   (c) Website C
   (d) Why ?
4. How would you improve the websites so that they are easier for children to use?
5. Did you like the tasks that you had to complete on three websites? Why?
6. On which of the three website did you find it most difficult to create the password? (images of the three sites shown to them)

(a) Website A

(b) Website B

(c) Website C

7. On which of the three website did you find it easiest to create the password?

   (a) Website A

   (b) Website B

   (c) Website C

8. Do you remember your passwords on three websites?

   (a) Yes

   (b) No (for which websites do you not remember your password)

      i. Website A

      ii. Website B

      iii. Website C

9. Do you think it would be easy for a stranger to guess the passwords you created on the websites? What about a friend or family member? Why?

10. Which of the three passwords you created would be the easiest for someone else to guess? Why?

    (a) Website A

    (b) Website B

    (c) Website C

11. Do you care if someone else has access to your online account? Why or why not? Who would be allowed?

Appendix F

Study 1: Password strength using the new strength measure

Participant	Condition	Password	Weaknesses	Strengths	New strength score
cs10	Medium complexity	Blanc111	- contains a dictionary word - predictable number pattern	- length greater than six characters - mixed character case - numbers	2
cs11	Medium complexity	Tamara04	- contains a user's name	- length greater than six characters - mixed character case - numbers	3
cs13	Medium complexity	Welcome2EV	- contains a dictionary word	- length greater than six characters - mixed character case - numbers	3
cs14	Medium complexity	Password1	- contains a dictionary word	- length greater than six - mixed character case - numbers	2
cs16	Medium complexity	Dsds456	- predictable number and character patterns	- mixed character case - numbers	3
cs17	Medium complexity	Azzybear1	- contains user's nickname - does not contain a special character	- length greater than six characters - mixed character case - numbers	3
cs18	Medium complexity	Jame16	- contains user's name	- mixed character case - numbers	2
cs19	Medium complexity	8a8s8d8f8g8h8j8k8L	- contains repeated number and a character pattern - does not contain a special character	- length greater than six characters - mixed character case - numbers	4
cs20	Medium complexity	Pandora1	- contains a dictionary word - does not contain a special character	- mixed character case - length greater than six characters	3
cs21	Medium complexity	Hmjt05	- does not contain a special character	- mixed character case - numbers	3
cs22	Medium complexity	jazsM611!	- none	- mixed character case - numbers - special character - length greater than six characters	5
cs23	Medium complexity	Bumblebee7	- contains a dictionary word - does not contain a special character	- mixed character case - numbers - length greater than six characters	3
cs24	Medium complexity	Alli_2005	- contains a name - contains year pattern	- mixed character case - numbers - special character - length greater than six characters	3

cs25	Medium complexity	Jullian5	- contains a user's name - contains a special character	- mixed character case - numbers - length is greater than six characters	2
cs4	Medium complexity	Camila8	- contains a user's name	- mixed character case - numbers - length greater than six characters	3
cs5	Medium complexity	Watermelon7	- contains a dictionary word	- mixed character case - numbers - length greater than six characters	2
cs6	Medium complexity	Kyles1	- contains a user's name	- mixed character case - numbers	2
cs7	Medium complexity	Haylie081!	- contains a user's name	- mixed character case - length greater than six characters - numbers - special character	3
cs8	Medium complexity	Stella123$	- contains a user's name	- mixed character case - length greater than six characters - numbers -special character	3
cs9	Medium complexity	Cs9222	- contains a predictable number pattern at the end	- mixed character case - numbers	3
cs10	High complexity	Blanc111!	- contains a dictionary word - contains a predictable number pattern	- mixed character case - length greater than six characters - numbers - special character	3
cs11	High complexity	Tam04!	- contains part of a user's name (Tammy)	- mixed character case - numbers - special character	4
cs13	High complexity	Welcome2EV!	- contain a dictionary word	- mixed character case - numbers - length is greater than six characters	4
cs14	High complexity	Password@223	- contain a dictionary word	- mixed character case - numbers - length is greater than six characters - special characters	3
cs16	High complexity	Ds34ter!	common number pattern	- mixed character case - numbers - special character - length is greater than six characters	5
cs17	High complexity	#Azzybear1	- contains user's nickname	- mixed character case - numbers - special character - length is greater than six characters	4
cs18	High complexity	Jame6!	- contains user's name	- mixed character case - numbers - special character	3

cs19	High complexity	Avabean1!	- contains user's nickname	- mixed character case - numbers - special character - length is greater than six characters	4
cs20	High complexity	Sillydog@100	- contains dictionary words	- mixed character case - numbers - special character - length is greater than six characters	3
cs21	High complexity	Hmjt05!	- none	- mixed character case - numbers - special character - length is greater than six characters	5
cs22	High complexity	Spain1!	- contains a dictionary word	- mixed character case - numbers - special character - length is greater than six characters	3
cs23	High complexity	Bumblebee61.	- contains a dictionary word	- mixed character case - numbers - special character - length is greater than six characters	3
cs24	High complexity	Alli_1234	- contains a name of a person - contains a common sequence of numbers	- mixed character case - numbers - special character - length is greater than six characters	3
cs25	High complexity	Jill5!	- contains user's name	- mixed character case - numbers - special character	3
cs4	High complexity	Camila11!	- contains user's name	- mixed character case - numbers - special character - length is greater than six characters	3
cs5	High complexity	Mr_Muffin7	- contains user's nickname	- mixed character case - numbers - special character - length is greater than six characters	3
cs6	High complexity	PRogamer2@	- contains a dictionary word	- mixed character case - numbers - special character - length is greater than six characters	3
cs7	High complexity	Haylie081!	- contains user's name	- mixed character case - numbers - special character - length is greater than six characters	3
cs8	High complexity	Stella123$	- contains user's name - contains a common sequence of numbers	- mixed character case - numbers - special character - length is greater than six characters	3

cs9	High complexity	cS9333*	- repeated sequence of numbers	- mixed character case - numbers - special character	4
cs10	Low complexity	blanc111	- contains a dictionary word - a repeated sequence of numbers - does not include uppercase characters - does not contain special character	- length/number	2
cs11	Low complexity	AY2902	- does not include lower case characters - does not include special characters	- uppercase characters - Numbers	2
cs13	Low complexity	Welcome2EV	- includes a dictionary word	- mixed character case - numbers - length is greater than six characters	3
cs14	Low complexity	Password1	- includes a dictionary word	- mixed character case - numbers - length is greater than six characters	2
cs16	Low complexity	ds345678	- includes a common sequence of numbers - does not include uppercase characters - does not include special characters	- numbers - length is greater than six characters	2
cs17	Low complexity	Azzybear1	- includes user's nickname - does not include special characters	- mixed character case - numbers - length is greater than six characters	3
cs18	Low complexity	jame6!	- includes user's name - does not include uppercase characters	- numbers - lowercase characters - special character	2
cs19	Low complexity	8a8s8d8f8g8h8j8k8l	- common sequence of number and alphabets - does not include special characters - does not include uppercase characters	- numbers - length is greater than six characters	3
cs20	Low complexity	SillyBillie	- includes dictionary words - does not include numbers - does not include a special character	- mixed character case	2
cs21	Low complexity	audrey	- includes a user's name - does not include special characters - does not include numbers - does not include uppercase characters	- lowercase characters	1
cs22	Low complexity	Spain1!	-includes dictionary words	- mixed character case - numbers - special characters - length greater than six characters	3
cs23	Low complexity	MarkStone61	- includes dictionary words - does not include special characters	- mixed character case - numbers - length greater than six characters	3

cs24	Low complexity	Alli_2005	name/year as number	- mixed character case - numbers - special character - length greater than six characters	3
cs25	Low complexity	1234567	- includes predictable number sequence - does not include mixed case characters - does not include special characters	- numbers	1
cs4	Low complexity	camila	- contains a user's name - does not include uppercase characters - does not include special characters - does not include numbers	- lowercase characters	1
cs5	Low complexity	watermelon	- includes a dictionary word - does not include uppercase characters - does not include special characters	- lowercase characters	1
cs6	Low complexity	kylese	- includes user's name - does not include uppercase characters - does not include special characters - does not include numbers	- lowercase characters	1
cs7	Low complexity	Haylie081!	- includes a user's name	- mixed character case - numbers - special character - length greater than six characters	3
cs8	Low complexity	Stella123$	- includes user's name - includes a common number sequence	- mixed character case - numbers - special character - length greater than six characters	3
cs9	Low complexity	CS9111	- includes a predictable number pattern - does not include special characters - does not include lowercase characters	- numbers - uppercase characters	2

Carleton UNIVERSITY
Canada's Capital University

Appendix G

Study 2: Informed Consent (Qualtrics)

Title: Evaluating parents' awareness of security and their children's password behaviors

Date of ethics clearance: 2017-08-08

REB clearance#: 107059

This study explores children's password behaviors, and parents' strategies to teach children about password security. The researcher for this study is Sumbal Maqsood, a Master's student in the School of Computer Science at Carleton University. She is working under the supervision of Prof. Sonia Chiasson and Prof. Robert Biddle in the School of Computer Science at Carleton University.

Task: The research study involves filling out a survey to provide information about yourself, your opinion on your children's password behaviors, threats that they are exposed to and the strategies you use to teach children how to stay safe online. The survey contains a few questions related to threats that your child is exposed to while online. Filling out the survey should take approximately 20 minutes.

Compensation: You will be compensated the amount you agreed upon before you entered into the survey. You will only receive compensation if you finish the survey.

Participation criteria: Parents of children aged 6-7, 8-9, 10-11, 12-13 years. The children should be regular internet users. Participants should live in Canada.

Risks: There are no known personal or physical risks associated with this survey. If you do choose to complete the survey, you will be able to skip questions if you choose. All research data will be password protected. The survey is being run by Qualtrics. The Qualtrics server is located in the U.S. and subject to U.S. laws on data privacy. All responses will be anonymous. Qualtrics will not collect participants IP addresses.

Withdrawal: You have the right to withdraw from the survey at any time, for any reason, up until you hit the "submit" button. You can withdraw by closing the

webpage containing the survey. If you withdraw from the study, your data will be deleted and not used for analysis. As the survey responses are anonymous, it is not possible to withdraw after the survey is submitted. Payment will not be issued if you withdraw from the study.

Data Use: The data collected through the survey may be accessed by the researcher and the research supervisors. Upon project completion, all research data will be kept in a password-protected format so that it may be compared to the results of other research related to this same topic. Results of the research may be used in research publications or for teaching purposes.

Clearance: The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

Researcher's contact information: Sumbal Maqsood,
Masters Student
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Email: sumbalmaqsood@cmail.carleton.ca

Supervisors' contact information:

Prof. Sonia Chiasson,
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Email: chiasson@scs.carleton.ca

Prof. Robert Biddle
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Email: robert_biddle@carleton.ca

Carleton UNIVERSITY
Canada's Capital University

Appendix H

Study 2: Recruitment poster (Qualtrics)

We are conducting an online survey to understand children's password behaviours and the strategies parents use to teach their children how to stay safe online. The survey is anonymous and should take approximately 20 minutes to complete. Participants will be informed prior to the start of the survey how will they be compensated.
Participants must be: *[first bullet will change depending on the age range for each group being recruited]*

- Parents with children of aged between 6 to 7, 8 to 9, 10 to 11, 12 to 13 years.
- The children must be regular Internet users.
- Participants should live in Canada.

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance#107059.

Researcher's contact information:
Sumbal Maqsood, Masters Student
School of Computer Science Carleton University
1125 Colonel By Drive, Ottawa, Ontario K1S 5B6
Email: sumbalmaqsood@cmail.carleton.ca

Supervisors' contact information:

Prof. Sonia Chiasson,
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Email: chiasson@scs.carleton.ca

Prof. Robert Biddle
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Email: robert_biddle@carleton.ca

Appendix I

Study 2: Survey - Evaluating parents' awareness of security and their children's password behaviors

Section 1 - Demographic information Children:

- How many children do you have?
- What is the age and gender of your child?
- What is the age and gender of your child?
- Age
- Gender
  - female
  - male
  - other
- Does this child have accounts on websites or mobile apps?

Parent:

- What is your age?
- You are a:
  - mother
  - father
  - guardian
  - other

- What is the highest level education you have completed?
  - high school diploma
  - college or Cegep
  - apprenticeship training (welder, electrician, hairstylist, plumber etc.)
  - post secondary (undergraduate degree)
  - post secondary (Masters or higher education)
  - other
- What is your current occupation?
- On which of the following websites or mobile apps do you have an account?
  - Social media
  - Email systems
  - News channels
  - Sports
  - Banking applications
  - Shopping websites
  - Other
- I don't have an account any websites or mobile apps
- How many hours do you spend online in a day across all of your devices?
- Approximately how many accounts do you have to online mobile apps or websites?

Section 2 - Understanding parents' awareness of security and their password practices

- When someone sends me a link, I open it without first verifying where it goes
  1. Never

2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- When browsing websites, I mouseover links to see where they go, before clicking them

1. Never
2. Rarely

3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- If I discover a security problem, I continue what I was doing because I assume someone else will fix it

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I do not change my passwords, unless I have to

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I use different passwords for different accounts that I have

1. Never
2. Rarely
3. Sometimes
4. Often

5. Always
6. Prefer not to answer

- When I create a new online account, I try to use a password that goes beyond the site's minimum requirements

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I do not include special characters in my password if it's not required

1. Never
2. Rarely
3. Sometimes
4. Often
5. Always
6. Prefer not to answer

- I have more than one password for different websites

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- I only have one password which I reuse across multiple websites:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Rate each password on how secure do you think it is:
    1. "WelcomeDEV2"
        (a) Least secure
        (b) Not secure
        (c) Neither secure or secure
        (d) Secure
        (e) Highly secure
        (f) Prefer not to answer
    2. "P@ssword!"
        (a) Least secure
        (b) Not secure
        (c) Neither secure or secure
        (d) Secure
        (e) Highly secure
        (f) Prefer not to answer
    3. "987654321"
        (a) Least secure
        (b) Not secure
        (c) Neither secure or secure

(d) Secure

(e) Highly secure

(f) Prefer not to answer

4. "hannah"

(a) Least secure

(b) Not secure

(c) Neither secure or secure

(d) Secure

(e) Highly secure

(f) Prefer not to answer

5. "Hmjt05!"

(a) Least secure

(b) Not secure

(c) Neither secure or secure

(d) Secure

(e) Highly secure

(f) Prefer not to answer

Section 3 - Parents' concerns about their child's password behaviours and the threats to which their child is exposed

- I am concerned about my child safety when they are online:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- I am concerned about my child:
- Being exposed to cyberbullying threats
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Talking to a stranger online (stranger danger)
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Sharing personal information online with others
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Getting involved in money related scams strongly disagree (1), disagree (2), neither agree nor disagree (3), agree (4), strongly agree (5) and prefer not to answer

- Being exposed to explicit content
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Using my personal information online
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- When creating a new account for my child:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- My child creates the account alone, but this makes me uncomfortable
    1. strongly disagree
    2. disagree

3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- My child creates the account alone, and I am comfortable with this action

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- I create the account for my child

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- We create the account together

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree

6. prefer not to answer

- My child re-uses the same passwords on multiple accounts

1. Always
2. Often
3. Sometimes
4. Rarely
5. Never
6. prefer not to answer

- I have shared one or more of my own passwords with my child:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- If "agree/strongly agree" (how do you decide which to share)

- My child has figured out/learned one or more of my passwords:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- I follow the recommended minimum age requirements for accounts on online websites or mobile apps for my children
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- How many passwords does your child have?
- Password creation rules:
    - I teach my child to create simple passwords that are easy to remember
        1. strongly disagree
        2. disagree
        3. neither agree nor disagree
        4. agree
        5. strongly agree
        6. prefer not to answer
    - I teach my child to create different passwords on different websites
        1. strongly disagree
        2. disagree
        3. neither agree nor disagree
        4. agree
        5. strongly agree
        6. prefer not to answer
    - I teach my child not to use their or my personal information in their passwords

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

- I teach my child to create passwords that are long (more than the minimum length)
  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer
- I teach my child to create passwords that are complex (uses special characters, numbers etc)
  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer

- What strategies do you use to help your child manage passwords?
  - I teach my child not to write down their password
  - I teach my child to write down their password and keep it in a safe place
  - I teach my child not to share their password with friends or strangers
  - I teach my child how to use a password manager to protect and manage their passwords

  - I teach my child to be careful when entering their passwords in public places (shoulder surfing)
  - Other

- Forgetting their passwords:
  - My child often forgets his/her password to online websites or mobile apps:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
  - My child resets the password by themselves when he/she forgets it:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
  - I reset the password for my child when he/she forget it:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer

- Strategies to remember passwords:
  - My child writes down his/her passwords to help remember them:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

– My child uses simple passwords that are easy to remember (for example, the password contains information such as their name, date of birth, nickname, favourite number, pet's name etc.) :

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

– My child tries to remember the password without writing it down or storing it on the computer/phone:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree
5. strongly agree
6. prefer not to answer

– My child shares accounts to websites or mobile apps with siblings:

1. strongly disagree
2. disagree
3. neither agree nor disagree
4. agree

5. strongly agree
6. prefer not to answer

Section 4 - Parents' beliefs and practices about creating passwords and practicing safe online behaviors

- I believe that my child is safe online:
  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer
- I think that my child creates secure passwords:
  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer
- I monitor my child's online activities:
  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree

6. prefer not to answer

- It is easy for me to monitor my child's online activities:

  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer

- I only allow my child to use an websites and mobile apps after first looking at it myself :

  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer

- I often talk to my child about the threats of being online, such as cyber bullying, stranger danger, scams etc.:

  1. strongly disagree
  2. disagree
  3. neither agree nor disagree
  4. agree
  5. strongly agree
  6. prefer not to answer

- I am concerned that my child's accounts could be hacked:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Children websites or mobile apps should require an account to login to interact with the mobile apps or websites:
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- Parental controls should be added on the child's devices (computer, phone, laptop):
    1. strongly disagree
    2. disagree
    3. neither agree nor disagree
    4. agree
    5. strongly agree
    6. prefer not to answer
- At what age do you think children should create their own passwords?
- At what age do you think children understand different password rules

- Password rules for children's accounts:
    1. Passwords rules should require uppercase letters
    2. Passwords rules should require lowercase letters
    3. Passwords rules should require numbers
    4. Passwords rules should require special characters
    5. Prefer not to answer
- What should be the minimum required password length for children's account?
- Who should teach children about password creation and management rules:
    - parent/guardian and family members
    - school
    - both parent/guardian/family members and school
    - Other
- What is the biggest risk to your child's accounts?
- Have you or has someone you know experienced an online attack (e.g., been hacked, scammed, bullied) ?
    - Yes
        * Can you tell us about it?
    - No
- Has your child experienced an online attack (e.g., been hacked, scammed, bullied) ?
    - Yes
        * Can you tell us about it?
    - No

- Is there a particular incident that has influenced your behaviour towards online security/safety?
- Do you have any other comments you'd like to share about this subject?

Appendix J

Study 2: List of participants' responses to question "What is the biggest risk to your child's accounts?"

- security
- Keyloggers
- getting hacked
- SOMEONE HACKING THEM AND FINDING OUT INFORMATION ABOUT MY CHILD
- To be hacked and they could try to get my information
- Just getting in with the wrong person, it would not be good.
- hacking
- being hacked
- bullies
- they do not know where they signing up to
- bullying
- Personal info being stolen
- being hacked
- being hacked
- they are hacked
- Friends hacking their accounts
- Giving out personal information or social hacking.
- being hacked
- hacked
- that he somehow wonders into sites he should not be going to.
- getting hacked
- hacking
- Sharing with friends
- they are hack easily
- hacked
- Just brief personal information.
- Her telling her password
- Hackers
- spending money
- HECKED
- unsafe content online
- Pedophiles
- inappropriate people contacting them
- OVERSPENDING
- someone will get their personal information

- bad websites
- LEAKAGE
- Being hacked and coming into contact with information/services/persons who are untrustworthy and/or lead to dangerous behaviour
- hacked
- Chatting with someone with bad motivation.
- getting hacked
- Scammers
- being hacked
- someone managing to figure out their password
- give to frind
- Being hacked
- cyber bullying
- CYBERBULLING
- that they should not share password with others
- hacking
- to encounter bad people
- other students in her school
- nothing i watch them like a hawk
- cyber bullies
- hacking
- Someone hacking it
- being hacked
- Spending money
- hacked
- pedophiles
- security
- perverts and cyber bullies but first and formost perverts
- ACESS TO INAPPROPRIATE
- cyber bullying
- HACKING
- HACKING
- Other malicioius users, whether online or in person.
- hacking
- SAFETY
- if they enter their address or photos
- password
- being exposed to inapropriate contente
- being hacked
- abuse
- Hacjers
- Identity Theft
- hackers
- hacking
- Bullying
- personal information

Appendix K

Study 2: Survey questions considered for the five composite variables

Below are the questions considered in computing a score for each of the five variables.

Participants' level of concern

- I am concerned about my child safety when they are online:
- I am concerned about my child:
  - Being exposed to cyberbullying threats
  - Talking to a stranger online (stranger danger)
  - Sharing personal information online with others
  - Getting involved in money related scams
  - Being exposed to explicit content
  - Using my personal information online
- I am concerned that my child's accounts could be hacked
- I monitor my child's online activities
- Children websites or mobile apps should require an account to login to interact with the mobile apps or websites
- I only allow my child to use an websites and mobile apps after first looking at it myself
- Parental controls should be added on the child's devices (computer, phone, laptop)

- I follow the recommended minimum age requirements for accounts on online websites or mobile apps for my children

Participants' belief in their child's password practices

- I think that my child creates secure passwords:
- My child re-uses the same passwords on multiple accounts
- My child has figured out/learned one or more of my passwords:
- Forgetting their passwords:
  - My child often forgets his/her password to online websites or mobile apps
  - My child resets the password by themselves when he/she forgets it:
  - I reset the password for my child when he/she forget it
- Strategies to remember passwords:
  - My child writes down his/her passwords to help remember them:
  - My child uses simple passwords that are easy to remember (for example, the password contains information such as their name, date of birth, nickname, favorite number, pet's name etc.) :
  - My child tries to remember the password without writing it down or storing it on the computer/phone:

Participants teaching secure passwords practices

- I teach my child to create simple passwords that are easy to remember
- I teach my child to create different passwords on different websites
- I teach my child not to use their or my personal information in their passwords
- I teach my child to create passwords that are long (more than the minimum length)

- I teach my child to create passwords that are complex (uses special characters, numbers etc)

Participants' level of awareness

- When someone sends me a link, I open it without first verifying where it goes
- I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar
- I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)
- When browsing websites, I mouseover links to see where they go, before clicking them
- If I discover a security problem, I continue what I was doing because I assume someone else will fix it

Participants' password creation practices

- I do not change my passwords, unless I have to
- I use different passwords for different accounts that I have
- When I create a new online account, I try to use a password that goes beyond the site's minimum requirements
- I do not include special characters in my password if it's not required
- I have more than one password for different websites
- I only have one password which I reuse across multiple websites: