View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Abertay Research Portal

Case Study – Exploring Children's Password Knowledge and Practices

Yee-Yin Choong
Mary Theofanos
Karen Renaud
Suzanne Prior

This is the authors' version of a paper presented at the Workshop on Usable Security and Privacy (USEC), 24th-27th February 2019, San Diego, which will be included in conference proceedings published by the Internet Society.

Case Study – Exploring Children's Password Knowledge and Practices

Yee-Yin Choong, Mary Theofanos
National Institute of Standards and Technology (NIST)
yee-yin.choong,mary.theofanos@nist.gov

Karen Renaud, Suzanne Prior
Abertay University, Dundee
k.renaud,s.prior@abertay.ac.uk

***Abstract*— Children use technology from a very young age, and often have to authenticate themselves. Yet very little attention has been paid to designing authentication specifically for this particular target group. The usual practice is to deploy the ubiquitous password, and this might well be a suboptimal choice. Designing authentication for children requires acknowledgement of child-specific developmental challenges related to literacy, cognitive abilities and differing developmental stages. Under-standing the current state of play is essential, delivering insights that inform the development of child-centred authentication mechanisms and processes. We carried out a systematic literature review of all research related to children and authentication since 2000. A distinct research gap emerged from the analysis. Thus, we designed and administered a survey to school children in the United States (US), so as to gain insights into their current password usage and behaviors. This paper reports preliminary results from a case study (part of a much larger research effort) of 189 children. The findings highlight age-related differences in children's password understanding and practices. We also discovered children having confusion between the concepts of safety and security. We conclude by suggesting directions for future research. This paper is work in progress.**

Keywords— Children, Passwords, Authentication, Perceptions

Introduction

Systems designed specifically for children are becoming increasingly popular. Many of these authenticate the child in order to retain a history of interaction, or to ensure that it is genuinely a child using the system. Usability testing with children is constrained by strict ethical requirements [59], [39], which might put researchers off testing alternative authentication mechanisms with this target group altogether. Without evidence of clearly superior and appropriate alternatives, it is understandable that developers revert to the password. This might well be a suboptimal choice for this user group due to issues such as heterogeniety in ability [87], language proficiency [57] and immature literacy [51]. Leaving developers without a viable alternative is no longer sustainable.

Most of the research in usable security has focused on adults. Yet, over the next 10 to 20 years the world's cyber posture and culture will be dependent on the cybersecurity and privacy knowledge and practices of today's youth. We performed a systematic literature review which high-lighted a lack of research examining extant child password use (Section II). Without an understanding of extant behavior, it is infeasible to start seeking an alternative, more appropriate, mechanism for child-tailored authentication. Thus, having identified this need, we proceeded to survey school children in the United States (US) to bridge this gap.

We reflect on our findings and suggest that we ought to prepare our children more effectively for a world where password hygiene is crucial. It is important enough to teach according to principles at a young age, and not

haphazardly, which the evidence suggests is being done at present. We deliberately nurture the development of good password hygiene habits as and when children are first learning to use their passwords, and introducing more advanced concepts as they develop and are able to adopt them. This would form the foundation for responsible adult password usage.

Systematic Literature Review

A rigorous literature search must be valid and reliable [94]. *Validity* is ensured by rigorously identifying: selected databases, keywords and inclusion and exclusion criteria; covered period; and applied forward and backward search. *Reliability* is based on the fully documented search process.

We searched through the following databases: Google Scholar[1], ACM, DBLP, IEEEXPlore, ScienceDirect and SpringerLink, http://worldcat.org PhD Theses, Educational literature: ERIC – Dept. of Education (Eric.ed.gov), Popular Press: Google News. We started off with Google Scholar and then augmented the list with articles from the other databases.

Key words: We used the following keywords for our search:

- Children/Minors/Teenagers/Adolescents and Authentication
- Children/Minors/Teenagers/Adolescents and Passwords
- Children/Minors/Teenagers/Adolescents and Security

Inclusion criteria: We chose to not only focus on high-quality literature and we also included lower rated journals, conferences and workshops as well as publications in the public media. We searched from the year 2000 onwards.

Exclusion criteria: We filtered out publications that were not written in English and those published before the year 2000, as well as patents.

Forward search: We used Google Scholar citation index service to perform a forward search.

Backward search: The backward search was conducted manually.

We conducted a full-text search, and the databases were searched to identify publications that contained at least one of the above combinations. We then applied the defined inclusion and exclusion criteria. Following this process only 87 publi-cations remained. Table I shows the number of publications for each database search, how many were excluded and how many remained for analysis. It should be noted that some publications appeared in more than one database.

TABLE I. OUTCOME OF LITERATURE SEARCH OF ALL DATABASES

Source	# papers	# eliminated	# retained
Google Scholar	65	13	52
ACM	2	0	2
DBLP	2	0	2
IEEEExplore	4	2	2
ScienceDirect	8	1	7
WorldCat	0	0	0
Eric	2	2	0
Google News	4	2	2
Scopus	4	1	3
Public Media	17	0	17

[1] Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

Findings

Table II summarizes the range of reports we analysed. Despite several of the retrieved papers considering new authentication methods, only four empirical studies were found which used children as participants in the development or evaluation of child-specific password systems [71], [16], [19], [54]. Of these, only Coggins [17] reported conducting a pre-study measure of the children's knowledge and experience of passwords. However, Coggins does not include information on what these pre-measures showed or what bearing they had on the final result.

TABLE II. CATEGORIES FROM ANALYSIS

Classification	**Refs**
Designing for Children	
Guidelines for keeping children safe online	[5], [13], [22], [25], [27], [35], [47], [64], [67], [73], [79], [80], [11], [37], [83], [24], [95], [49], [50], [40], [84], [66], [6], [77],
Argument for children's privacy	[8], [86]
Study of children's Internet Usage	[15], [32], [36], [45], [55], [82], [85], [44], [49], [23], [21], [48], [78], [43], [61], [62], [63], [16], [58], [69], [74], [81], [75], [76],
Accessibility Issues	[29]
Security awareness	[2], [9], [31], [46], [69], [70], [91], [33], [88], [89], [93], [52], [17], [53], [65], [92]
Children Accessing Adult Content	[96], [72]
Children & Authentication	
Proposes new authentication ideas	[61], [38], [18]
Empirical Study of Passwords and Children	[42], [71], [54], [41]
Empirical Evaluation of Child-Specific Authentication Methods	[71], [16], [19], [54]
Designing Security for children	[30], [68], [26]
Anecdotal reports of children's password behaviors	[1], [10], [7], [20], [28]
Children & Biometrics	[4], [90]
Proposes new authentication ideas	[60], [38], [18]

This literature review revealed a gap in the literature related to gauging current levels of comprehension and practice related to passwords. Filling this gap is important because researchers conducting empirical studies in this area benefit from understanding the current level of password knowledge held by children and indeed some indication of their current password practices.

Research Methodology

Given the limited work to date in measuring children's knowledge and experience of passwords, there is a need for more studies to add to these findings in different contexts. In this study, we developed a self-report survey to understand what challenges children grades 3 through 12 face regarding passwords. The goal was to identify students' practices, perceptions, and knowledge regarding passwords. Each student answered questions assessing their use of computers, passwords, password practices, knowledge about and feelings about passwords, together with information about grade and gender. We wanted to address the following research questions (RQ):

RQ1. How do children currently use Computers and Passwords?

RQ2. Password Understanding:

a. Password Hygiene Knowledge?

b. Why do they need passwords?

c. What are students' passwords perceptions?

d. Do they know how to create a strong password?

RQ3. Password Behaviors:

a. How do students select, remember and store passwords?

b. What are the characteristics of the password they are asked to formulate to access a game?

The survey was administered to grades 3 through 12 in six school districts in the Southeast, South and Midwest in the US.

Survey Development

The research questions guided the development of objectives for accessing student's use of computers, of passwords, password practices, knowledge about passwords, feelings about passwords, and tests for gender, age and school differences. A list of possible items was generated targeting the objectives as illustrated in the alignment matrix in the Appendix.

Two surveys were designed: one 15 item survey for grades 3 to 5, and a 16 item survey for grades 6 to 12. All of the items were closed response except for four open response items where students were asked: how many passwords they have; how many times a day they use passwords; to list a reason(s) why people should use passwords, and to generate a new password for a given scenario.

While the surveys were identical in item content, the language and format of the response variables were tailored for appropriateness to the age groups. For example, most of the response variables were "Yes" or "No" for the 3rd – 5th graders, while the 6th – 12th graders' response variables were lists of check all that apply.

To ascertain the content and construct validity of the survey instruments, four types of reviews were conducted. *Content experts* in usable security were asked to evaluate the alignment matrix (in the Appendix) and provide feedback on the alignment of the categories with the scope of the survey goals, of the alignment of the items with the category, and if there were missing items. *Survey experts* also reviewed each item for clarity for the intended audience, appropriate format for what the item is assessing, and alignment of response options. *Content experts* (elementary, middle and high school teachers) focused on the language and format of the items based on the grade/age of the students. *Cognitive interviews* with students, to determine if the questions were indeed being interpreted as intended, were also conducted using a talk-aloud protocol. Cognitive probing techniques where students were asked to both paraphrase items (e.g., "How would you ask the question in your own words") and interpret them (e.g., "What is your answer and why") complemented the talk-aloud protocol. Additionally, we piloted the surveys with students. After each type of review, the survey instruments were refined based on the feedback and comments.

Procedure & Recruitment

The study was approved by the full Institutional Review Board. Principals and teachers were recruited to participate. The schools, individual teachers, and students that participated were compensated. Each school received $1000, the

teachers received $50 gift cards, and the students received age appropriate trinkets such as caricature erasers, ear buds as examples. Finally, parental consent and student assent forms were collected prior to survey distribution. Students who did not receive parental consent performed alternative activities following the school's standard protocol during the survey administration. Each participating classroom also received $50 for a classroom thank-you celebration where all students celebrated, including those who did not participate in the survey. The survey administration was tailored for the appropriate age group. All children completed scantron survey forms, with teachers reading the survey aloud in the 3rd – 5th grades.

The results presented here are the initial results from only two US Midwest schools – an elementary (3rd – 5th grades) and a middle school (6th – 8th grades). This is the first data set from a much larger research effort that will include between 1500 to 1800 elementary, middle and high school students from up to six US school districts.

Participants

In this case study dataset, a total of 189 school students completed the surveys. Both schools are located in the Midwest region in the US. Table III presents the participant demographics.

TABLE III. PARTICIPANT DEMOGRAPHICS

Grades	**#**	**Gender** F- female M- male U- unspecified	**Age** (Years)		
			Range	$\overline{x}$	**SD**
3rd – 5th	88	53.41% (F) 42.05% (M) 4.54% (U)	8-12	8.15	0.96
6th – 8th	101	51.49% (F) 40.59% (M) 7.92% (U)	11-15	12.55	1.03

results

RQ1: Current Usage

Current Computer Usage

The most popular type of computers the 3rd – 5th graders use was gaming console (80.68%), followed by laptop (78.41%) and tablet (71.59%). For the 6th – 8th graders, the most popular type of computers was cell phone (87.13%), followed by laptop (80.20%) and gaming console (77.23%). Table IV is a list of all types of computers used by the participants in the survey.

TABLE IV. USAGE OF DIFFERENT TYPES OF COMPUTERS

	Desktop	Laptop	Tablet	Cell phone	Gaming console
3rd – 5th	62.50 %	78.41 %	71.59 %	68.18 %	80.68 %
6th – 8th	64.36 %	80.20 %	55.45 %	87.13 %	77.23 %

Locations where students use the computers were mostly at school or at home: the 3rd – 5th graders reported computer use at school (98.86%) and at home (81.82%); the 6th – 8th graders reported similar computer use at school (94.06%) and a higher usage at home (91.09%).

Activities that students use computers for ranged from school work, homework to games and social media. Games (92.05% for 3rd – 5th and 84.16% for 6th – 8th) and entertainment (89.77% for 3rd – 5th and 85.15% for 6th – 8th) were the most popular activities on computers for both groups. Table V is a list of computer activities sorted by 3rd – 5th graders' percentages. Percentages of 6th – 8th graders follow a similar pattern.

Table V. Activities using Computers sorted by 3rd – 5th graders' percentages

	3rd – 5th	**6th – 8th**
Games	92.05%	84.16%
Entertainment	89.77%	85.15%
Internet	80.68%	77.23%
School	75.00%	78.22%
Texting	45.45%	56.44%
Social media	43.18%	63.37%
Email	36.36%	35.64%
Homework	32.95%	55.45%

Current Password Usage

On average (medians), the 3rd – 5th graders have 2 passwords at school and 3 passwords at home. They reported to use their passwords about 4 times a day. For the 6th – 8th graders, they have on average (medians) 2 passwords at school and 4 passwords at home; use passwords about 4 times a day.

More than 90% in both groups reported that they use passwords to access school computers, and between about 71% to 80% reported using passwords to unlock home computers. Table VI lists technologies locked with passwords reported by participants in the survey.

Table VI. What Children Authenticate to Use

	3rd – 5th	**6th – 8th**
School computers	98.86%	94.06%
Home computers	71.59%	80.20%
Tablets	60.23%	55.45%
Cell phones	62.50%	85.15%
Games	55.68%	40.59%
Email	29.55%	45.54%
Social media	45.45%	69.31%

RQ2: Understanding of Password Hygiene

Knowledge

The 3rd – 5th graders reported learning about good password use more at home (71.59%) compared to at school (38.64%); whereas the 6th – 8th graders reported learning with almost equal percentages at school (73.27%) and at home (76.24%).

Regarding what they know about password hygiene, responses of "*Always*" and "*Sometimes*" were combined, shown in Table VII. More than 90% of each age group reported that they keep their passwords private; and they keep a good habit of signing out after computer use (89.77% for the 3rd – 5th graders and 94.06% for the 6th – 8th graders). The 6th – 8th graders tend to share their passwords with friends more.

Table VII. Knowledge of Password Hygiene

	3rd – 5th	**6th – 8th**
Keep passwords private	90.91%	93.70%
Sign out after computer use	89.77%	94.06%
Share with friends	32.95%	47.52%
Use same password for everything	57.95%	78.22%
Change passwords	62.50%	79.21%

For those who reported that they changed their passwords, the top reasons were "*when someone finds out my passwords*" (94.55% for the 3rd – 5th graders and 72.50% for the 6th – 8th graders) and "*when I forgot my passwords*" (54.55% for the 3rd – 5th graders and 68.75% for the 6th – 8th graders).

Why Passwords?

Both groups of participants were asked why it is important to use passwords. The 3rd – 5th graders were only asked to provide one reason while the 6th – 8th graders were asked to provide up to three reasons.

These responses were independently analysed by two authors using thematic coding. The authors met and agreed on the final codes. The agreed codes were at a very high level, reflecting the relatively concise answers given by the children. For example: "*To keep things safe*", "*Safety*", and "*People should use passwords so they can have privacy*".

The final codes are shown in Table VIII; codes with fewer than 5 responses are not included. The higher number of responses attributed to codes within the 6*th* — 8*th* graders are due to a higher number of participants and this group being asked to provide three responses, as opposed to one.

Table VIII. Coding of Survey Responses

3rd – 5th (n, % of responses)	**6th – 8th** (n, % of responses)
Privacy (34, 40.48%)	Privacy (81, 38.02%)
Safety (18, 21.42%)	Safety (41, 19.24%)
Access (15, 17.85%)	Security (40, 18.77%)
Security (9, 10.71%)	Access (24, 11.27%)
Hacking (6, 7.14%)	Hacking (10, 4.69%)

Password-Related Perceptions

The 3rd – 5th graders reported higher percentages of perceiving creating and remembering passwords as easy, than the 6th – 8th graders, as shown in Table IX. Both age groups found it fairly easy to enter passwords with a keyboard or using a touch screen. Although having too many passwords does not seem to be bothersome to either group, we do see a rising trend with older children having more passwords as they get older.

Table IX. Perception of Passwords

	3rd – 5th	**6th – 8th**
Easy to make my password	76.14 %	54.46 %
Easy to make many different passwords	61.36 %	44.55 %

Easy to remember my passwords	80.68 %	68.32 %
Easy to enter my passwords with a keyboard	77.27 %	80.20 %
Easy to enter my passwords on a touch screen	71.59 %	81.19 %
I wish there was another way besides passwords.	50.00 %	31.68 %
I have too many passwords.	27.27 %	16.83 %

RQ3: Password Behaviors

Password Selection & Storage

When asked about how they get their passwords, about 85% in both age groups reported getting some passwords from schools.

Younger students (3rd – 5th graders) reported a high percentage of parental involvement in creating their passwords (either created by parents or they created their own passwords with help from parents, combined: 69.32%). A high percentage of the 6th – 8th graders (86.14%) reported creating their own passwords and low parental involvement (either created by parents or created their own passwords with help from parents, combined: 35.64%).

Participants reported memorizing their passwords (97.73% for the 3rd – 5th graders and 91.08% for the 6th – 8th graders). About a third of students in each group reported that they write passwords on paper. The 3rd – 5th graders also reported higher percentages relying on external sources (such as auto-fill by computer, family members remember for me, or save in a file on computer) compared to the 6th – 8th graders. Table X is a list of mechanisms of how students remember passwords.

Table X. How Students RETAIN Passwords

	3rd – 5th		**6th – 8th**
	Always[2]	*Sometimes*	*Check all apply*
Memorize	78.41 %	19.32%	91.09 %

[2] Response variables were tailored for age-appropriateness for this question: "*Always*," "*Sometimes*," and "*Never*" for the 3rd – 5th graders; whereas the 6th – 8th graders got the entire list and were asked to "*check all that apply*."

Let computer save the password and auto-fill	32.95 %	31.82%	36.63 %
Write passwords down on paper	12.50 %	23.86%	33.66 %
Family member remembers for me	6.82 %	28.41%	9.90%
Friend remembers for me	2.27 %	7.95%	1.98%
Save in a file on computer	10.23 %	87.50%	12.87 %

The 6th – 8th graders were asked an additional question on whether they help their family members with passwords. Forty-Nine students (48.51%) reported "*Yes*," – of those, 73.47% reported helping family members to remember their passwords.

Created Password Analysis

The two groups were asked: "*Let's say you just got a new game to play on the computer, but you need a password to use it. Please make up a new password for that game. (Remember, don't write down one of your real passwords.)*".

Password Characteristics

The average (medians) lengths of the passwords created by participants were: 7 characters for the 3rd – 5th graders, with a range of [3, 32]; and 10 characters for the 6th – 8th graders, with a range of [4, 29]. Lowercase letters make up the majority of the passwords, followed by numbers. The most popular characters used were lowercase letters "a," "e," and "o" for the 3rd – 5th graders and "e," "a," and "r" for the 6th – 8th graders. The most used numbers for both age groups were "1" and "2." Symbols or white spaces were rarely used. Figure 1 shows the distribution of different character types used in the passwords created by the participants.

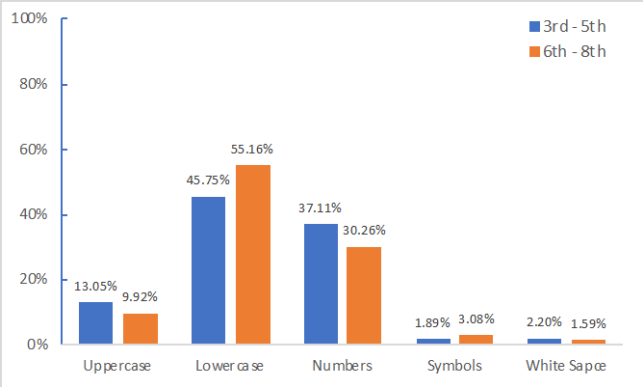

Fig. 1. Character Types in Passwords

We further examined character type positioning in the passwords. Figures 2 and 3 display the overall character type distribution relative to their position, for password lengths of 7 (for the 3rd – 5th graders) and password lengths of 10 (for the 6th – 8th graders).

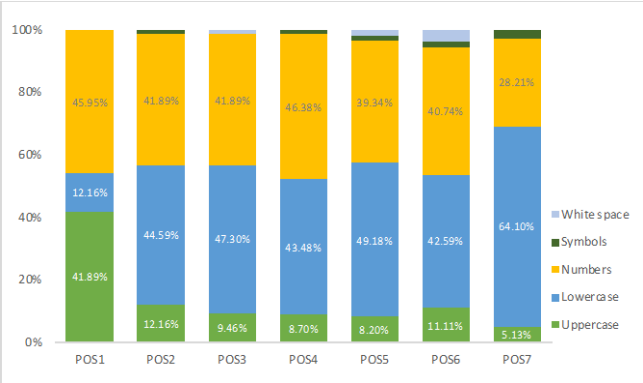

Figure 2: Character Types by Positions in Passwords (3^{rd} – 5^{th})

As shown in Figure 2, in general, the percentages of the 3^{rd} – 5^{th} students who used lowercase letters and numbers were very close (around 40%) across all positions except for the two ends, i.e. position 1 (POS1) and position 7 (POS7). In POS1, 41.89% of the 3^{rd} – 5^{th} graders used uppercase letters in their passwords. In position 7, a lot more 3^{rd} – 5^{th} graders (64.10%) included lowercase letters in their passwords.

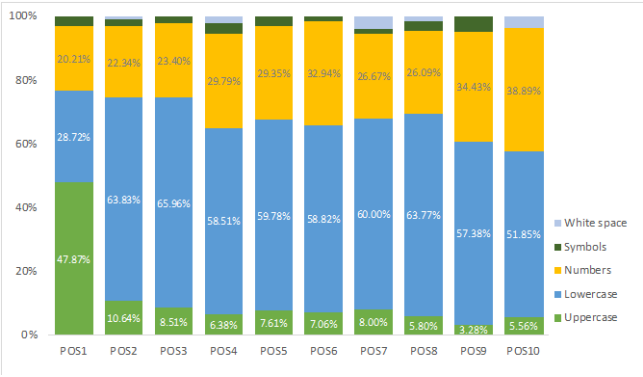

Figure 3: Character Types by Positions in Passwords (6^{th} – 8^{th})

In contrast, the pattern for the 6^{th} – 8^{th} graders (Figure 3) looks quite different from that for the 3^{rd} – 5^{th} graders. A lot more 6^{th} – 8^{th} graders (between 52% and 64%) used lowercase letters across all positions except for the first position. Much fewer 6^{th} – 8^{th} students (between 20% and 39%) used numbers in their passwords compared to their younger counterparts. Similar to the 3^{rd} – 5^{th} graders, in POS1, 47.87% the 6^{th} – 8^{th} graders included uppercase letters in their passwords.

Password Strength

We used the zxcvbn.js JavaScript Library[3] to quantify the strength of the passwords the children formulated. Figure 4 shows the strengths of the two groups' passwords. There is an improvement as the children move up in the educational system, but the percentage of very weak passwords is still very high, even amongst the older group.

[3] https://www.bennish.net/password-strength-checker/

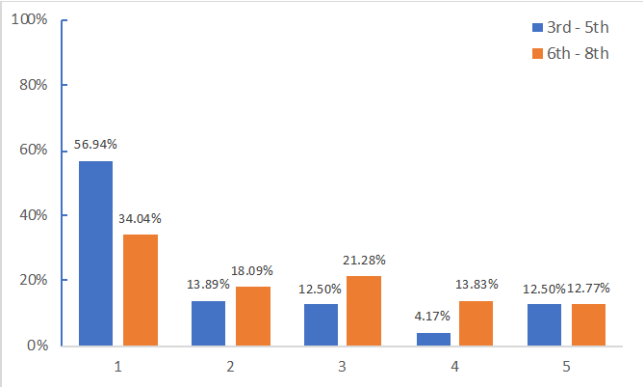

Fig. 4. Password Strengths

Discussion, Reflection and Recommendations

RQ1: Password & Computer Usage

Not surprisingly, as children age, their use of technology and on-line activities change. The percentages of students having cell phones increases almost 20% from the younger to the older children, as shown in Table IV. As the children mature, there is also about a 10% increase in some social activities, with texting increasing, and about a 20% increase in social media (in Table V). As a result, the older children experience more and more needs for authentication: about 23% increase in cell phone authentication, 15% increase in email authentication, and 24% increase in social media authentication (Table VI). The increase needs for authentication for older children translates into having more passwords, each of which has to be retained and managed.

RQ2: Password Knowledge

Children demonstrated a confusion between the concepts of passwords, privacy and safety or protection. Many children reported believing that passwords would keep them 'safe': "*I think that people should use passwords because it saves everyone's lives*" (Female, 3^{rd} — 5^{th} grader)

Similar feelings were expressed in 22% of the younger group's responses and 19% of the elder group. This suggests that the message that passwords are required for security is becoming confused either in the delivery or in the children's receiving of the message with the idea of safety, forming inaccurate mental models. It is not clear why this is happening but scaring children into using passwords is unlikely to be the most effective method for ensuring they continue to develop good cyber security practices as they age. Resources in the area of cyber security for children are often focused on cyber bullying and the dangers of online predators, which may explain where some of the confusion arises from. Although educators and parents may not be intentionally trying to scare children into using passwords, children are receiving mixed messages. This demonstrates a need for clear and consistent messages. In order to achieve this is may be necessary to provide additional training to those delivering the message, in this case parents and teachers.

RQ3: Password Practices and Behaviors

Children's ages influence their password practices and behaviors. Younger children rely more on their family in creating and remembering passwords. Almost twice as many of the younger group reported having parental help in creating their passwords. And, about 35% of the younger children reported getting help from family members in remembering their pass-words, as compared to only 10% of the older children.

Parents also play an important role of providing guidance on 'good' password hygiene to the younger group. In contrast, schools play a larger role in influencing password behaviors of the older group. Moreover, the older children assist family members with remembering passwords. Both age groups understand that passwords should remain private and they sign out after computer use. However, approximately 50% of the older group reported sharing passwords friends.

Reflection

These findings raise several questions. How do we best prepare children for the increasing demands of living with passwords? How do we provide guidelines and strategies as they age to learn and develop appropriate skills?

A. Password Management Lifecycle

It is necessary to consider users' password behaviors in a holistic manner, realizing that there are three stages in password management lifecycle – password creation, password maintenance, and authentication. Users' behaviors are reflections of the interactions among stages in the lifecycle, the capabilities and limitations of the human information processor, and the individual factors [14]. Each stage requires cognitive capabilities from the password owner, in this case the child, to create, maintain, and authenticate using passwords. Overall, the 6^{th} – 8^{th} graders reported experiencing more difficulties with their passwords. Approximately 20% more of the 6^{th} – 8^{th} graders than the 3^{rd} – 5^{th} graders reported difficulties in *creating* passwords (Table IX). They also struggled more to *maintain* their passwords: 20% more of the older group reported using "same password for everything" (Table VII), probably because about 12% more of the older children found it difficult to remember passwords (Table X). It is important not to consider any of the lifecycle stages in isolation when we design authentication mechanisms for a particular target group, such as children.

B. Password Choice

On average, the 6^{th} – 8^{th} graders created passwords that were 3 characters longer than the 3^{rd} – 5^{th} graders did. Compared to the 6^{th} – 8^{th} graders, the 3^{rd} – 5^{th} graders used more uppercase letters, numbers, and white spaces when composing their passwords. The 3^{rd} – 5^{th} graders tend to start their passwords with numbers or uppercase letters in the 1^{st} position. Immediately after the 1^{st} position, lowercase letters and numbers dominate the next few positions until towards the end of the password where almost 2/3 of the characters are lowercase letters. The 6^{th} – 8^{th} graders also tend to start their passwords with uppercase letters, but numbers are not dominating as in the case of their younger counterparts. Immediately after the 1^{st} position, the 6^{th} – 8^{th} graders use much higher percentage of lowercase letters than any other character types in all positions. Towards the end positions in the password, we observe slight rising trends of using numbers and symbols. In a password generation study with 81 adults [56], the researchers found that uppercase letters dominate the 1^{st} position in the password, then the rate of uppercase letters sharply drops at the 2^{nd} position, while the lowercase letters substantially rise at position 2. Numbers follow a steady increasing trend and start dominating towards the latter positions in the password, until the last position where symbols make up half of the character distribution. The 6^{th} – 8^{th} graders' password trend resembles patterns of uppercase, lowercase, numbers, and symbols found in passwords generated by adults. This could be due to the fact that as students get older, they have more exposure to password complexity requirements for numbers and symbols.

The passwords that the participants created did not use a broad range of characters. For the 3^{rd} – 5^{th} graders, only 8 characters appeared with frequency higher than or equal to 3%, namely, 2, 1, a, e, o, 3, 5, and 6. For the 6^{th} – 8^{th} graders, only 11 characters appeared with frequency higher than or equal to 3%, namely, 2, e, 1, a, r, o, 4, n, l (lowercase), i and s. Special character use was very scarce in passwords created by the 3^{rd} – 5^{th} graders. There was some increasing usage of special characters by the 6^{th} – 8^{th} graders. Many passwords consist of concepts reflecting the current state of the children's lives, e.g., fairy tales, numbers, colors, games, and sports. Few examples from

passwords created by the 3rd – 5th graders are: “12345,” “Yellow,” “PrincessFrog248,” and “doggysafesecure.” Some passwords created by the 6th – 8th graders are: “Gamehead77,” “GameGuy007,” “Basketball1130,” and “Blue101213.” The simplistic nature of passwords is expected since students are progressing on their literacy levels as they age. This is especially true with younger students who are working on mastering their alphabets and numbers. Special characters are such a foreign concept to many young students. This is evidenced by the fact that only 6 special characters appeared in the passwords created by the 3rd – 5th graders, namely, dash (-), period (.), exclamation (!), question (?), at sign (@), and underscore (_), with frequencies all under 1%. The usage of special characters did expand to more types with the 6th – 8th graders: exclamation (!), slash (/), period (.), comma (,), underscore (_), double quote (“), at sign (@), apostrophe (’), left and right parentheses ( ), and caret (^), with frequencies all under 1%.

Despite the awareness shown when discussing the purposes of passwords, the passwords chosen by the children (particularly by the younger age group) were very weak. There were some improvements in the older group, but, as a whole, the passwords were not strong. This suggests that children are not choosing weak passwords because they do not understand the importance of protecting themselves online but because they are either unaware of what constitutes a strong password, or are unable to generate one. There is clearly a need to address how children, particularly in the younger age group, understand and use passwords. When considering the strength of password required it may be worth considering what it is that is being protected and how strong a password is needed. While there have been several investigations into alternative methods of authentication for children, as yet none have been widely adopted. It is important that we do not make passwords “too easy” for children to use leading to their resisting more complicated passwords as adults. The password demands need to challenge children, while still being achievable. Traditional password requirements would suggest that the complexity and strength required should increase as the child’s ability develops. However, new password guidelines published by the National Institute of Standards and Technology (NIST) suggests encouraging longer passwords (passphrases) while relaxing complexity requirements (i.e., not requiring a combination of different character types) [34].

Conclusion and Future work

Users’ password behaviors and experiences across all three stages in the password lifecycle influence users’ attitudes and perception toward password use and requirements, it is important to promote positive user attitudes early on. Users holding positive attitudes towards passwords practice better cyber hygiene, such as creating compliant and strong passwords, writing down passwords less often, suffering less frustration with authentication, better understanding and respecting the significance of security, as compared to users with negative attitudes [14]. This suggests the need to encourage young users to develop positive attitudes and accurate mental models of passwords and authentication.

It is already well known that children are not a homogenous group and frequently studies involving children as participants in designing or evaluating new software products will take into consideration their literacy or numeracy skills. This study suggests that despite growing up with an awareness of cyber security, children are likely to have had widely different experiences and knowledge surrounding passwords. As such, researchers working in the areas of authentication should ensure they measure this existing skill and knowledge base when conducting studies with this population.

It is very important that, when we teach children about passwords, we do not confuse them. There are important differences between security, privacy and safety and it is worth finding ways of communicating these differences to children as they learn about password practice and hygiene. They need to understand the differences between password security, information privacy and online safety. We do not want to make children afraid of cyber security and we want them to understand their privacy rights. This is a huge challenge but needs urgent attention.

This paper reports the preliminary findings of a case study from two Midwest schools. We are currently collecting data from other planned US school districts. We plan to perform thorough statistical analysis on the entire dataset of 1500 to 1800 students to further validate the findings in this paper and increase generalizability.

References

[1] 3rdknight. Password complexity for primary school, 2010. edugeek 7 May http://www.edugeek.net/forums/windows/55683-password-complexity-primary-school.html.

[2] A. E. M. Aloufi. A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years. Master's thesis, Rochester Institute of Technology, 2015.

[3] N. Alqahtani, S. Furnell, S. Atkinson, and I. Stengel. Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi Context. In *Internet Technologies and Applications (ITA)*, pages 98–103, Sept 2017.

[4] Anonymous. Biometrics - it's all child's play! *Biometric Technology Today*, 15(5):7–8, 2007.

[5] A. L. Bair. Implementing a digital family policy, March 2015. USA Today.

[6] S. Bauman and H. Pero. Bullying and cyberbullying among deaf students and their hearing peers: An exploratory study. *Journal of deaf studies and deaf education*, 16(2):236–253, 2011.

[7] BBC. Xbox password flaw exposed by five-year-old boy, 2014. http://www.bbc.co.uk/news/technology-268791854April.

[8] I. R. Berson and M. J. Berson. Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education*, 21(1):135–147, 2006.

[9] I. B. Bovina, N. V. Dvoryanchikov, and S. V. Budykin. Shared meanings about information security of children: An exploratory study. *Procedia-Social and Behavioral Sciences*, 146:94–98, 2014.

[10] D. Boyd. How Parents Normalized Teen Password Sharing, 2012. http://www.zephoria.org/thoughts/archives/2012/01/23/January 23.

[11] C. Chang. Internet safety survey: Who will protect the children. *Berkeley Tech. Law Journal*, 25:501–527, 2010.

[12] S. Chaudron. Young children (0-8) and digital technology. *A qualitative exploratory study across seven countries. Joint Research Centre. European Commission*, 2015.

[13] A. D. Cheok, O. N. N. Fernando, and C. L. Fernando. Petimo: safe social networking robot for children. In *Proceedings of the 8th International Conference on Interaction Design and Children*, pages 274–275. ACM, 2009.

[14] Y.-Y. Choong. A cognitive-behavioral framework of user password management lifecycle. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 127–137. Springer, 2014.

[15] J. Clarke. The Internet according to kids. *Young Consumers*, 3(2):45–52, 2002.

[16] P. E. Coggins III. Implications of what children know about computer passwords. *Computers in the Schools*, 30(3):282–293, 2013.

[17] P. E. Coggins III. A pedagogical example of second-order arithmetic sequences applied to the construction of computer passwords by upper elementary grade students. *International Journal of Mathematical Education in Science and Technology*, 46(3):441–450, 2015.

[18] J. Cole, G. Walsh, and Z. 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.

[19] J. Cole, G. Walsh, and Z. 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, 2017.

[20] Daily Mail. Eight in ten children know the passwords and PIN codes to their parents' laptops, phones and computers, May 2013. http://www. dailymail.co.uk/news/article-2328193/.

[21] D. Daramola. Young Children as Internet Users and Parents Perspec-tives. Master's thesis, University of Oulu, 2015.

[22] G. Davis. Bringing up the next generation of digital citizens, 2015. https://blogs.mcafee.com/consumer/family-safety-survey-results/.

[23] T. S. P. D. de Castro. *"It's a complicated situation". Harm in everyday experiences with technology. A qualitative study with school-aged children*. PhD thesis, Universidade do Minho, 2015.

[24] J. F. DeFranco. Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers (J1)*, 86(5):52–55, 2011.

[25] S. Dredge. How do I keep my children safe online? What the security experts tell their kids, 2014. The Guardian.

[26] A. Druin. Lifelong interactions designing online interactions: what kids want and what designers know. *interactions*, 15(3):42–44, 2008.

[27] G. Fahrnberger, D. Nayak, V. S. Martha, and S. Ramaswamy. Safechat: A tool to shield children's communication from explicit messages. In *14th International Conference on Innovations for Community Services (I4CS)*, pages 80–86. IEEE, 2014.

[28] C. Farivar. This 11-year-old is selling cryptographically secure passwords for $2 each, 2015. http://arstechnica.com/business/2015/10 Ministry of Innovation / Business of Technology.

[29] J. Feng, J. Lazar, L. Kumin, and A. Ozok. Computer usage by children with down syndrome: Challenges and future research. *ACM Transactions on Accessible Computing (TACCESS)*, 2(3):13:1–13:44, 2010.

[30] J. Fruth, R. Merkel, and J. Dittmann. Security warnings for children's smart phones: A first design approach. In *Communications and Multimedia Security*, pages 241–243. Springer, 2011.

[31] J. Fruth, C. Schulze, M. Rohde, and J. Dittmann. E-learning of it security threats: A game prototype for children. In *Communications and Multimedia Security*, pages 162–172. Springer, 2013.

[32] S. Furnell. Getting past passwords. *Computer Fraud & Security*, 2013(4):8–13, 2013.

[33] V. Ginodman, N. Obelets, R. Herkanaidu, R. Reid, and J. Van Niekerk. Snakes and ladders for digital natives: information security educa-tion for the youth. *Information Management & Computer Security*, 22(2):179–190, 2014.

[34] P. Grassi, E. Newton, R. Periner, A. Regensheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y.-Y. Choong, K. Greene, and M. Theofanos. Digital identity guidelines: Authentication and lifecycle management. Technical Report 800-63B, NIST Special Publication, 2017.

[35] J. Guan and J. Huck. Children in the digital age: exploring issues of cybersecurity. In *Proceedings of the 2012 iConference*, pages 506–507. ACM, 2012.

[36] A. L. Gutnick, M. Robb, L. Takeuchi, and J. Kotler. Always connected: The new digital media habits of young children, 2011. Sesame Workshop and the Joan Ganz Cooney Center.

[37] A. Hajirnis. Social media networking: Parent guidance required. *The Brown University Child and Adolescent Behavior Letter*, 31(12):1–7, 2015.

[38] B. A. Handler. Method and system for child authentication, Mar. 10 2015. US Patent 8,978,130.

[39] L. Hanna, K. Risden, and K. Alexander. Guidelines for usability testing with children. *interactions*, 4(5):9–14, 1997.

[40] B. Holfeld and B. J. Leadbeater. The nature and frequency of cyber bullying behaviors and victimization experiences in young canadian children. *Canadian Journal of School Psychology*, 30(2):116–135, 2015.

[41] K. Hundlani, S. Chiasson, and L. 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.

[42] A. Imran. *A comparision of Password Authentication Between Children and Adults*. PhD thesis, Carleton University Ottawa, 2015.

[43] L. A. Jackson, R. Samona, J. Moomaw, L. Ramsay, C. Murray, A. Smith, and L. Murray. What children do on the Internet: Domains visited and their relationship to socio-demographic characteristics and academic performance. *CyberPsychology & Behavior*, 10(2):182–190, 2006.

[44] C. Johnston. Social media is parents' greatest online fear, research says, 2014. The Guardian, 12 November.

[45] A. Julka, G. Stehr, D. Parks, and D. Trechter. Student use of communication technologies —- parent/guardian survey report, March 2010. Survey Research Center Report 2010/8 http://www.uwrf.edu/SurveyResearchCenter/loader.cfm?csModule=security/getfile&PageID=27599.

[46] L. T. Karklins. *The risks of social networking sites to South Australian high school students*. PhD thesis, Flinders University of South Australia, School of Law., 2013.

[47] J. Kim, K. Kim, J. Park, and T. Shon. A scalable and privacy-preserving child-care and safety service in a ubiquitous computing environment. *Mathematical and Computer Modelling*, 55(1):45–57, 2012.

[48] L. Kimmerly and D. Odell. Children and computer use in the home: Workstations, behaviors and parental attitudes. *Work*, 32(3):299–310, 2009.

[49] K. Kopecky`. Czech children and facebook–a quantitative survey. *Telematics and Informatics*, 33(4):950–958, 2016.

[50] K. Kopecky`. Misuse of web cameras to manipulate children within the so-called webcam trolling. *Telematics and Informatics*, 33(1):1–7, 2016.

[51] G. Kress. Before writing: Rethinking the pathway into writing, 1997.

[52] E. Kritzinger. Enhancing cyber safety awareness among school chil-dren in South Africa through gaming. In *Science and Information Conference (SAI), 2015*, pages 1243–1248. IEEE, 2015.

[53] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vi-tak. 'no telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW):64:1–64:21, Dec. 2017.

[54] D. R. Lamichhane and J. 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.

[55] M. A. Lauri, J. Borg, and L. Farrugia. Children's Internet Use and Parents' Perceptions of their Children's Online Experience. A study commissioned by the Malta Communications Authority.

[56] P. Y. Lee and Y.-Y. Choong. Human generated passwords–the impacts of password requirements and presentation styles. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 83–94. Springer, 2015.

[57] W. Loban. *The language of elementary school children.* National Council of Teachers of English, Champaign, IL, 1963.

[58] B. Lorenz, K. Kikkas, and A. Klooster. "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In *Human Aspects of Information Security, Privacy, and Trust*, pages 276–283. Springer, 2013.

[59] S. MacFarlane, J. Read, J. Höysniemi, and P. Markopoulos. Half-day tutorial: Evaluating interactive products for and with children. In *Interact*, pages 1027–1028, 2003.

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

[61] D. J. Meter and S. Bauman. When sharing is a bad idea: the effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology, Behavior, and Social Networking*, 18(8):437–442, 2015.

[62] F. Mishna, M. Saini, and S. Solomon. Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review*, 31(12):1222–1228, 2009.

[63] A. Mubarak, O. Judy, and Z. Harrison. Bridging the gap between adolescents and adults: A case study on experiences of teenagers while using social networking sites and their willingness to seek adult help. *International Journal of Computer Applications*, 102(6):36–42, 2014.

[64] B. Nansen, K. Chakraborty, L. Gibbs, C. MacDougall, and F. Vetere. Children and Digital Wellbeing in Australia: Online regulation, conduct and competence. *Journal of Children and Media*, 6(2):237–254, 2012.

[65] L. Pangrazio and N. Selwyn. 'My data, my bad. ..'-Young people's personal data understandings and (counter) practices. In *Proceedings of the 8th International Conference on Social Media & Society*, July 28–30, Toronto, ON, Canada, 2017.

[66] P. Paul. Cracking teenagers' online codes. *The New York Times*, 20, 2012.

[67] Y. Poullet. e-Youth before its judges–Legal protection of minors in cyberspace. *Computer Law & Security Review*, 27(1):6–20, 2011.

[68] J. C. Read and R. 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.

[69] J. C. Read and B. Cassidy. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, pages 200–203. ACM, 2012.

[70] R. Reid and J. van Niekerk. A cyber security culture fostering campaign through the lens of active audience theory. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance*, pages 34–44, Lesvos, Greece, 1-3 July 2015.

[71] K. Renaud. Web authentication using Mikon images. In *Privacy, Security, Trust and the Management of e-Business, 2009. Congress'09. World Congress on*, pages 79–88. IEEE, 2009.

[72] K. Renaud and J. Maguire. Regulating access to adult content (with privacy preservation). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 4019– 4028. ACM, 2015.

[73] M. Ribble. *Raising a Digital Child: A Digital Citizenship Handbook for Parents*. International Society for Technology in Education, 1st edition, 2009.

[74] M. Richtel. Young, in love and sharing everything, including a password, 17 January 2012. http://www.nytimes.com/2012/01/18/us/teenagers-sharing-passwords-as-show-of-affection.html.

[75] K. Rim. Investigation and analysis of password use for the betterment of privacy protection education in middle and high school students. *Advanced Science and Technology Letters*, 103:72–76, 2015.

[76] K. Rim and S. Choi. Analysis of password generation types in teenagers–focusing on the students of jeollanam-do. *International Journal of u-and e-Service, Science and Technology*, 8(9):371–380, 2015.

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

[78] A. Samuel. Your Weakest Security Link? Your Children. http://www.wsj.com/articles/your-weakest-security-link-your-children-1429499471 Wall Street Journal, 19 April.

[79] M. Sharples, R. Graber, C. Harrison, and K. Logan. E-safety and web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning*, 25(1):70–84, 2009.

[80] C. A. Shoniregun and A. Anderson. Is Child Internet Access a Questionable Risk? *Ubiquity*, 2003(September):4:1–4:1, Sept. 2003.

[81] E. Stobert and R. Biddle. Authentication in the home. In *Workshop on Home Usable Privacy and Security*, 2013.

[82] J. D. Sutter. Survey: 70% of teens hide online behavior from parents, 2012. http://www.cnn.com/2012/06/25/tech/web/mcafee-teen-online-survey/.

[83] T. Swist, P. Collin, J. McCormack, A. Third, and W. Australia. *Social media and the wellbeing of children and young people: A literature review*. Commissioner for Children and Young People, 2015.

[84] İ. Tanrıkulu, S. A. Altun, Ö. E. Baker, and O. Y. Güneri. Misuse of icts among turkish children and youth: A study on newspaper reports. *International Journal of Human Sciences*, 12(1):1230–1243, 2015.

[85] M. Teimouri, M. S. Hassan, J. Bolong, A. Daud, S. Yussuf, and N. A. Adzharuddin. What is upsetting our children online? *Procedia-Social and Behavioral Sciences*, 155:411–416, 2014.

[86] A. D. Thierer. Kids, privacy, free speech & the Internet: Finding the right balance. https://papers.ssrn.com/sol3/papers.cfm?abstractid=1909261., 2011.

[87] C. A. Tomlinson. *How to differentiate instruction in mixed-ability classrooms*. Association for Supervision and Curriculum Development, Alexandria, Virginia., 2nd edition, 2001.

[88] A. Trinneer. Teaching children about Internet safety: An evaluation of the effectiveness of an interactive computer game. Master's thesis, School of Psychology, University of Ottawa (Canada), 2006.

[89] S. J. Tsim. Internet safety education: Information retention among middle school aged children. Master's thesis, San Jos´e State University, 2006.

[90] A. Uhl and P. Wild. Comparing verification performance of kids and adults for fingerprint, palmprint, hand-geometry and digitprint biometrics. In *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems,(BTAS)*, pages 1–6, 2009.

[91] S. Vandoninck and L. d'Haenens. Children's online coping strategies: Rethinking coping typologies in a risk-specific approach. *Journal of adolescence*, 45:225–236, 2015.

[92] T. Velki, K. Solic, V. Gorjanac, and K. Nenadic. Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. In *2017 40th International Conven-tion on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1280–1284, May 2017.

[93] M. Villano. Text unto others... as you would have them text unto you, September 2008. https://thejournal.com/articles/2008/09/01/text-unto-others-as-you-would-have-them-text-unto-you.aspx.

[94] J. Vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *ECIS*, volume 9, pages 2206–2217, 2009.

[95] J. Weed. Online monitoring: Do you know your child's passwords?, 2011. 28 March https://www.parentmap.com/article/online-monitoring-do-you-know-your-childs-passwords.

[96] H. Zaikina-Montgomery. *The dilemma of minors' access to adult content on the Internet: A proposed warnings solution*. PhD thesis, University of Nevada, Las Vegas, 2011.

Appendix: Survey Alignment Matrix

Objective	Category	Category Definition	Survey Items
RQ1: **Assess students' use of computers**	usage	Extent to which students use computers	• What types of computers do you use? • Where do you use computers? • About how much time do you spend on computers each day during the week? • About how much time do you spend on computers during the weekend? • What do you do when you go on the computer? (list of activities)
RQ1: **Assess students' use of passwords**	usage	Extent to which students use passwords	• How many passwords do you have? • I use passwords to login into (list of activities). • How many times a day do you use or enter your passwords?

RQ2:
 	
Assess students' knowledge of passwords
	knowledge	Extent to which students understand purpose and appropriate security practices with passwords	• Where did you learn about good password use?
			• Let's talk about your passwords:
			  ○ Do you share your password with friends?
			  ○ Do you use the same password for everything?
			  ○ Do you write your password down on paper?
			  ○ Do you change your passwords?
			  ○ When do you change your passwords?
			  ○ When you finish with the computer do you log out?
			• List up to 3 reasons why we need passwords?

RQ2:
 	
Assess students' feeling about passwords
	perceptions	Extent to which students are comfortable with passwords and password practices	• What do you think of passwords (scales of agreement):
			  ○ It is easy to create my password.
			  ○ It is easy to create many different passwords.
			  ○ It is easy to remember my passwords.
			  ○ It is easy to type in my passwords.

			○ I wish there was another way to login besides passwords. ○ I have too many passwords.
RQ3: **Assess students' current password practices**	behaviors	Extent to which students are self-reliant with respect to passwords	• How do you pick your password? • How do you remember your passwords? • Do you help your family members with passwords? (6^{th} – 12^{th} graders only) • Let's say you just got a new game to play on the computer but you need a password to use it. Please make up a new password for that game.
Test for gender, age and school differences.	demographics	Age, gender, school, grade	• Are you a girl or boy, prefer not to answer? • How old are you? • What grade are you in? • Where do you go to school? • Which city do you live in?