JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–19
doi: 10.1093/cybsec/tyz015
Research paper

Research paper

"Passwords protect my stuff"—a study of children's password practices

Yee-Yin Choong [1,*], Mary F. Theofanos[1], Karen Renaud[2] and Suzanne Prior[2]

[1]National Institute of Standards and Technology, Gaithersburg, MD, USA; [2]School of Design and Informatics, Abertay University, Dundee, UK

*Correspondence address: National Institute of Standards and Technology, Gaithersburg, MD 20899, USA. Tel: +1-301-975-3248; E-mail: yee-yin.choong@nist.gov

Received 26 June 2019; accepted 29 October 2019

Abstract

Children use technology from a very young age and often have to authenticate. The goal of this study is to explore children's practices, perceptions, and knowledge regarding passwords. Given the limited work to date and that the world's cyber posture and culture will be dependent on today's youth, it is imperative to conduct cyber-security research with children. We conducted surveys of 189 3rd to 8th graders from two Midwest schools in the USA. We found that children have on average two passwords for school and three to four passwords for home. They kept their passwords private and did not share with others. They created passwords with an average length of 7 (3rd to 5th graders) and 10 (6–8th graders). But, only about 13% of the children created very strong passwords. Generating strong passwords requires mature cognitive and linguistic capabilities which children at this developmental stage have not yet mastered. They believed that passwords provide access control, protect their privacy and keep their "stuff" safe. Overall, children had appropriate mental models of passwords and demonstrated good password practices. Cyber-security education should strive to reinforce these positive practices while continuing to provide and promote age-appropriate developmental security skills. Given the study's sample size and limited generalizability, we are expanding our research to include children from 3rd to 12th graders across multiple US school districts.

Key words: children; passwords; authentication; perceptions; password practices

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 the child using the system. Usability testing with children is constrained by strict ethical requirements [1, 2], 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 heterogeneity in ability [3], language proficiency [4], and immature literacy [5].

Most of the research in usable security has focused on adults. Yet, over the next 10–20 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 'Systematic literature review'). 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 USA 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 should deliberately nurture the development of good password hygiene habits as and when children are first learning to use their passwords. We should introduce 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

We previously published a paper that included a systematic literature review [6]. We briefly mention our findings here for the sake of completeness.

Table 1 provides an over of the categories the reviewed papers fitted into. Despite several of the reviewed papers considering new authentication methods, only four empirical studies were found that specifically used children as participants in the development or evaluation of child-specific authentication [7–10]. Of these, only Coggins [11] 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.

The 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. Hence, our previous paper [6] was a first step into this direction.

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?

Survey development

The research questions guided the development of objectives for accessing student's use of computers, 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 Table 2.

Two surveys were designed: one 15-item survey for grades 3–5, and a 16-item survey for grades 6–12. 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 graders 3–5, while the graders' 6–12 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 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. The final surveys were converted to Scantron compatible forms (in the Appendix).

Procedure and recruitment

The study was approved by the full Institutional Review Board (IRB). Principals and teachers were recruited to participate. The schools, individual teachers, and students that participated were

Table 1: categories from literature review

Designing for children		Children & authentication	
Classification	Number of papers	Classification	Number of papers
Guidelines for keeping children safe online	25	Proposes new authentication ideas	3
Argument for children's privacy rights	2	Empirical study of passwords and children	4
Study of children's Internet usage	25	Empirical evaluation of child-specific authentication methods	4
Accessibility issues	1	Designing security for children	3
Security awareness	15	Anecdotal reports of children's password behaviors	5
Children accessing adult content	2	Children and biometrics	2

Table 2: 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? (6–12th 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?

compensated. Each school received $1000, the teachers received $50 gift cards, and the students received age appropriate trinkets such as caricature erasers or ear buds, for example. 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 to 5th grades. The data were collected anonymously. Each completed survey was assigned a unique participant ID, for example, P0001.

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

Table 3: participant demographics

Grades	#	Gender (%)			Age (Years)		
		Girl	Boy	Unspecified	Mean	SD	Range
3rd to 5th	88	53.41	42.05	4.54	8.15	0.96	8–12
6–8th	101	51.49	40.59	7.92	12.55	1.03	11–15

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 USA. Table 3 presents the participant demographics.

Table 4: usage of different kinds of computers

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

Table 5: activities using computers

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

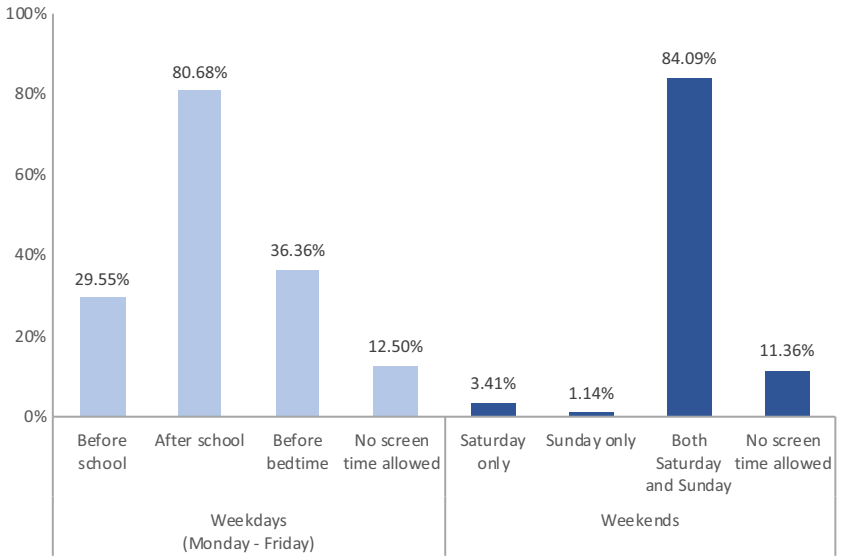

Figure 1: Screen time allowed (3rd to 5th).

Results

RQ1: Current usage

Current computer usage

The most popular type of computers the 3rd to 5th graders use was gaming console (80.68%), followed by laptop (78.41%), and tablet (71.59%). For the 6–8th graders, the most popular type of computers was cell phone (87.13%), followed by laptop (80.20%), and gaming console (77.23%). Table 4 is a list of all types of computers used by the participants in the survey.

Locations where students use the computers were mostly at school or at home: the 3rd to 5th graders reported computer use at school (98.86%) and at home (81.82%); the 6–8th 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 to 5th and 84.16% for 6–8th) and entertainment (89.77% for 3rd to 5th and 85.15% for 6–8th) were the most popular activities on computers for both groups. Table 5 is a list of computer activities sorted by 3rd to 5th graders' percentages. Percentages of 6–8th graders follow a similar pattern.

For 3rd to 5th graders, they were allowed to have screen time mostly "after school" (80.68%) during weekdays; screen time was allowed for both Saturday and Sunday (84.09%), as shown in Figure 1. For 6–8th graders, only about 20% of them spent screen time of more than 5 hours each day during weekdays, but more than 40% of the students reported spending screen time for more than 5 hours per day on weekends (Figure 2).

Current password usage

On average (medians), the 3rd to 5th graders have two passwords at school and three passwords at home. They reported to use their passwords about four times a day. For the 6–8th graders, they have on average (medians) two passwords at school and four passwords at home; use passwords about four times a day. More than 90% in both groups reported that they use passwords to access school computers, and between about 71% and 80% reported using passwords to unlock home computers. Table 6 lists technologies locked with passwords reported by participants in the survey.

RQ2: Understanding of password hygiene

Knowledge

The 3rd to 5th graders reported learning about good password use more at home (71.59%) compared to at school (38.64%), whereas the 6–8th 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 7. More than 90% of each age group reported that they keep their passwords private; and they keep a good habit of signing out after

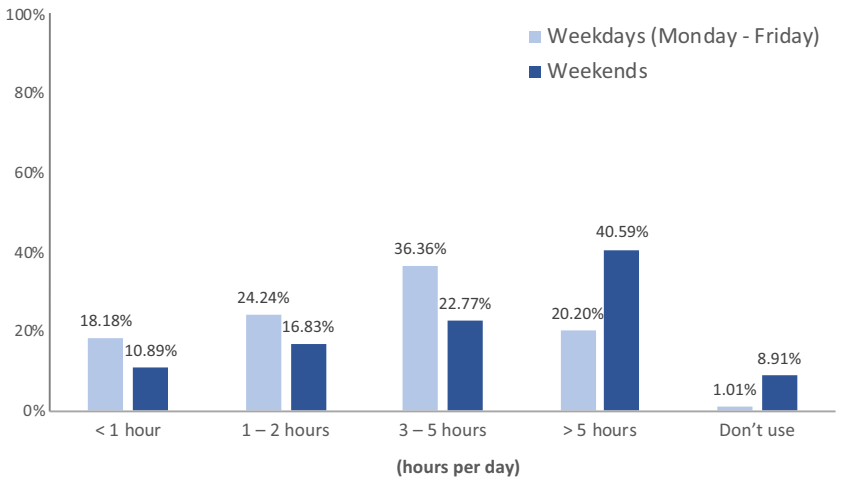

Figure 2: Screen time spent (6–8th).

Table 6: what children authenticate to use

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

Table 7: knowledge of password hygiene

	3rd to 5th (%)	6–8th (%)
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

computer use (89.77% for the 3rd to 5th graders and 94.06% for the 6–8th graders). The 6–8th graders tend to share their passwords with friends more.

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

Why passwords?

Both groups of participants were asked: "Why do you think people should use passwords?" The 3rd to 5th graders were only asked to provide one reason while the 6–8th graders were asked to provide up to three reasons.

The responses for "Why do you think people should use passwords?" were analyzed by two members of the research team. Each member independently analyzed the responses using thematic coding and identified codes and sub-codes. The team members met to merge and discuss the codes. The codes were revised and operationalized based on the discussions, ensuring that both points of view were captured. The new codes were applied and fully operationalized. The final code names incorporated the terminology and language that the students used for example "stuff" as a sub-code. There were seven top level codes and 15 sub-codes. The final code book of top-level codes is shown in Table 8.

Table 8: qualitative analysis code book – top codes

Codes	Code operationalization
Access control	Mentioned the ability (i.e., allow access) or inability (i.e., prevent access) to use such as accounts, devices, data, information
Hacking	Mentioned *hack* (literally), or *scam*
Privacy	Mentioned *private*, *privacy*, *confidentiality*, or *secret* (literally)
Protection	Mentioned *protect* or *protection* (literally); to avoid loss (such as data/information, devices, finances/money); concerned with personal or physical protection
Safety	Mentioned *safe* or *safety* (literally), or mentioned *track*(*ing*), *stalk*(*ing*), *cyberbully*, or *kidnap*; concerned with online harm from bad people; concerned with personal or physical safety
Security	Mentioned *secure* or *security* (literally)
Steal	Mentioned *steal*, *stolen*, or *theft* (literally)

As shown in Table 9, "Access control" was the most frequently provided reason for why passwords. Students' responses included both preventing access and providing access. Example responses were "To keep people out of their stuff" (P745, 3rd) and "So you can get into your account or device" (P2880, 6th). "Privacy" was the second-most common reason cited. Examples from the students include "To keep stuff private" (P2918, 8th), and "To keep your private information to yourself" (P811, 5th). Safety was another big category of responses: "To keep their stuff safe" (P2966, 7th) and "... because someone might track you down" (P 691, 3rd) are representative of this category. "Protection" was the last major category cited: reasons included "To protect their stuff" (P2855, 6th) and "To be protected" (P2893, 6th). The remaining three categories of hacking, steal, and security completed the list. For "Hacking", students responded with "So someone doesn't hack them" (P2970, 8th) and "... people can hack in your stuff" (P685. 4th). Responses such

as "So people won't steal your account" (P2968, 8th) and "if someone steals your phone" (P2940, 7th) were common themes in the "Steal" category. Finally, "Security" was the least common reason for using passwords, examples include: "to keep your stuff secure" (P2946, 7th) and "it gives your device security" (P2919, 8th).

As evidenced by these quotes, "stuff" emerged as a popular subcode across all of the primary codes. The 3rd to 5th graders referred to "stuff" in 25.88% of their responses while the 6–8th graders used "stuff" in 41.00% of the time.

Password-related perceptions

The 3rd to 5th graders reported higher percentages of perceiving creating and remembering passwords as easy, than the 6–8th graders, as shown in Table 10. 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.

RQ3: Password behaviors

Password selection and storage

When asked about how they get their passwords, about 85% in both age groups reported getting some passwords from schools. Younger students (3rd to 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 6–8th 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 to 5th graders and 91.09% for the 6–8th graders). About a third of students in each group reported that they write passwords on paper. The 3rd to 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 6–8th graders. Figure 3 shows mechanisms of how students remember passwords.

The 6–8th 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: seven characters for the 3rd to 5th graders, with a range of (3, 32); and 10 characters for the 6–8th graders, with a range of (4, 29). A nonparametric Wilcoxon rank

Table 9: coding of survey responses.

	3rd to 5th (%)	6–8th (%)
Access control	48.24	89.00
Privacy	25.88	59.00
Safety	18.82	40.00
Protection	3.53	23.00
Hacking	7.06	13.00
Steal	2.35	13.00
Security	0.00	9.00

Table 10: perception of passwords

	3rd to 5th (%)	6–8th (%)
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

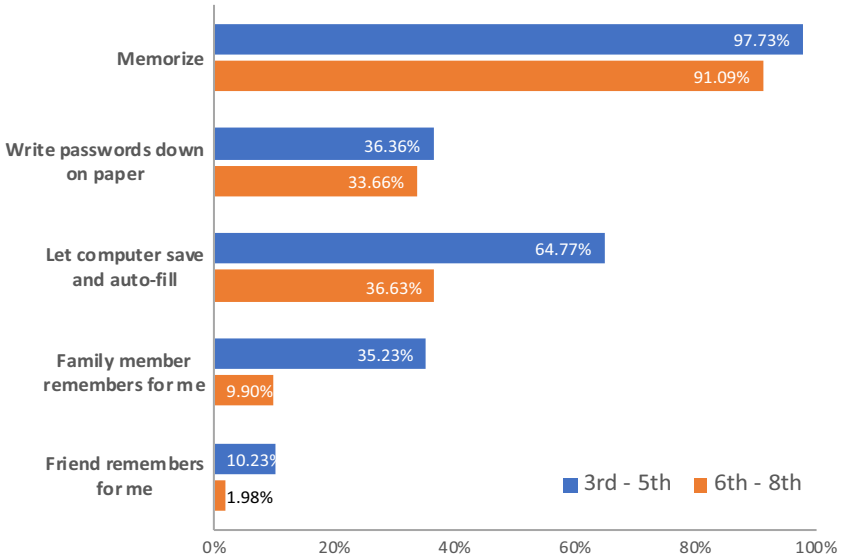

Figure 3: How children retain passwords.

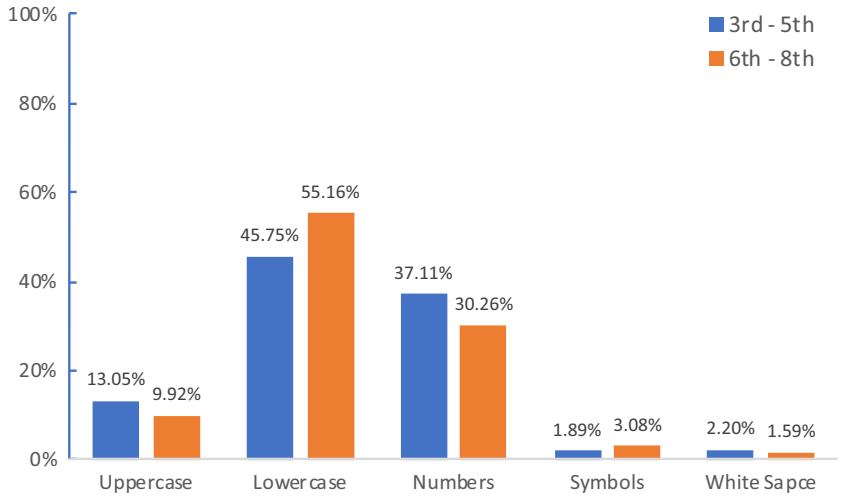

Figure 4: Character types in passwords.

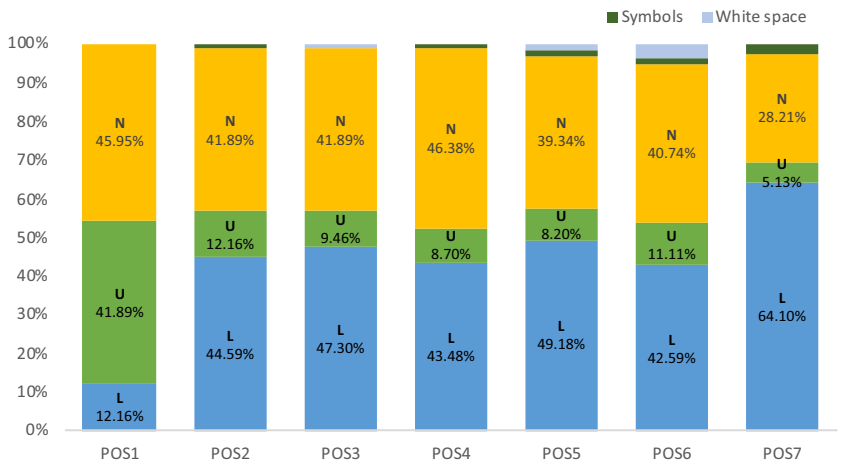

Figure 5: Character types by positions in passwords (3rd to 5th).

(L—lowercase, U—uppercase, N—numbers)

sum test comparing the average password lengths between the two age groups shows that they are significantly different ($W = 2318$, $P < 0.05$).

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 to 5thgraders and "e," "a," and "r" for the 6–8th graders. The most used numbers for both age groups were "1" and "2". Symbols or white spaces were rarely used. Figure 4 shows the distribution of different character types used in the passwords created by the participants.

We further examined character type positioning in the passwords. Figures 5 and 6 display the overall character type distribution relative to their position, for password lengths of 7 (for the 3rd to 5th graders) and password lengths of 10 (for the 6–8th graders). As shown in Figure 5, in general, the percentages of the 3rd to 5th 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 3rd to 5th graders used uppercase letters in their passwords. In position 7, a lot more 3rd to 5th graders (64.10%) included lowercase letters in their passwords.

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

Password strength. For the purpose of our study, we decided to measure password strength with the password strength meter which uses the zxcvbn.js[1] script. This is an open-source tool, which uses pattern matching and searches for the minimum entropy of a given password. While we investigated the use of other password strength assessment tools, we were limited to tools that do not retain password data in order to comply with our IRB requirements.

The score rating provided by zxcvbn.js measures password strength on an ordinal scale with "0" being assigned to a password

1 https://www.bennish.net/password-strength-checker/

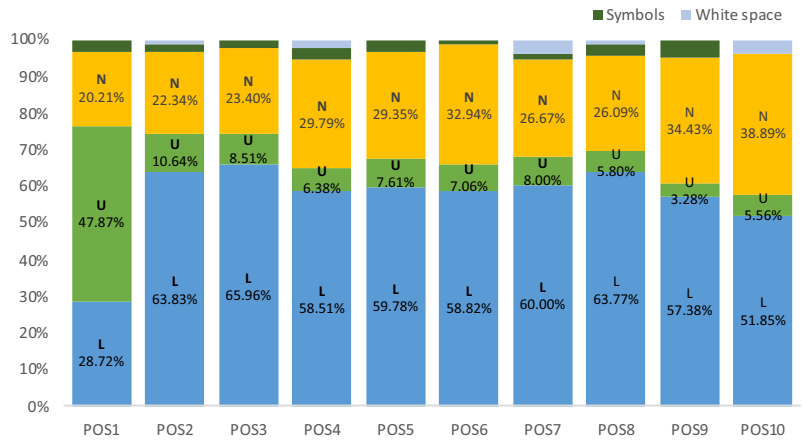

Figure 6: Character types by positions in passwords (6–8th).

(L—lowercase, U—uppercase, N—numbers)

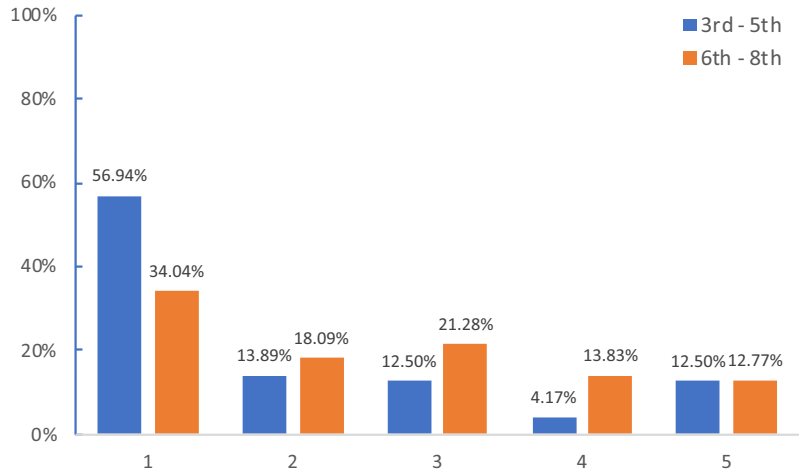

Figure 7: Password strength.

that can be guessed within 100 guesses. A "4" is assigned to a password that required over 10 to the power of 8 guesses. Collapsing password strength to a 5-item ordinal scale undeniably suppresses data variance. For example, if the number of guesses to crack one password was 1100 and the estimated number of guesses for another password is 9900, both passwords would be assigned a rating of 2. Yet, there is a large difference in the number of guesses and the identical rating does not reflect this. Figure 7 shows the strengths of the two groups' passwords.

The percentages of very weak passwords (i.e., score of 1) are high for both age groups. Children used all numbers or simple common words in the passwords that were assigned a score of 1, for example, 3rd to 5th—"1260", "Yellow" and "Game 1234"; 6–8th—"12345", "happydays" and "Fridneship2". Only about 13% of children from each age group were able to create strong passwords with a score of 5, for example, "Puppy uppy gamer 15." and "dancingdinosaursavrwhoop164".

Discussion

RQ1: Password and computer usage

Not surprisingly, as children age, their use of technology and online activities change. The percentages of students having cell phones increases almost 20% from the younger to the older children, as shown in Table 4. 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 5). As a result, the older children experience more and more need for authentication: about 23% increase in cell phone authentication, 15% increase in email authentication, and 24% increase in social media authentication (Table 6). The increased need for authentication for older children translates into their having more passwords, each of which has to be retained and managed.

RQ2: Password knowledge

Overall the children understood that passwords provide a means of access control both to provide access to legitimate users and to deny access to others as Figures 8 and 9 clearly demonstrate. It is not surprising that following the top-level code of access control, safety and privacy were dominant themes. Generation Z (Gen Z), those born from the mid-1990s to the late 2000s (the population in this case study) have several unique generational characteristics that influence their behavior [12, 13]. Many of these characteristics directly influence their password perceptions and behaviors.

First, Gen Z'ers are digital natives, living in a fully digital world where interaction with technologies require authentication.

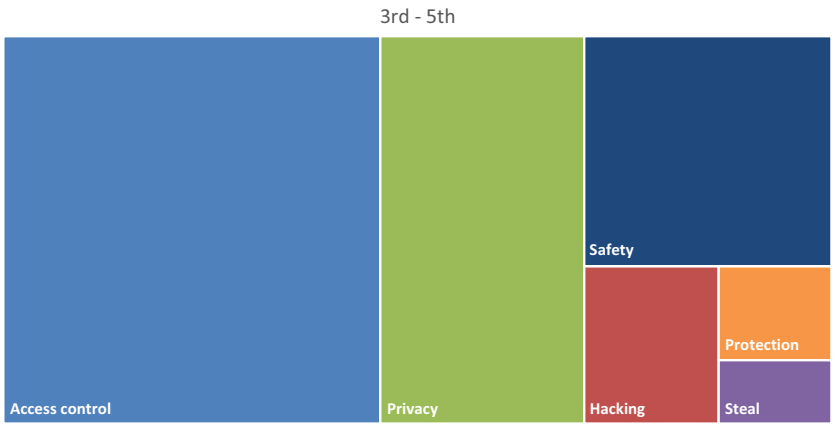

Figure 8: Why passwords? (3rd to 5th).

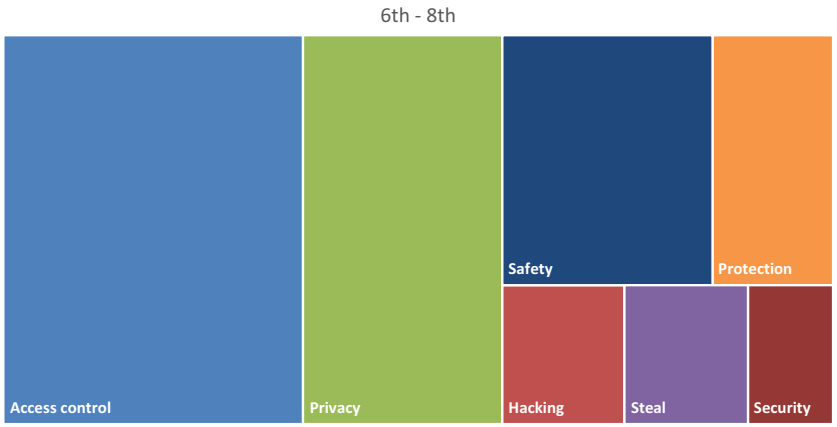

Figure 9: Why passwords? (6–8th).

They are the first generation who have not lived through a change from analog to digital. All of the technologies and electronics are just part of their normal life.

Second, "the world they live in has never felt safe" [13]. Most are too young to remember or were born after the 11 September 2001 terrorist attacks. They have always known international terrorism and school shootings. Much like technology, this is the norm for them rather than the exception. Given this background, citing safety as a response to the need for passwords makes sense.

Finally, Gen Z'ers value their privacy [13]. This generation has witnessed the digital privacy mistakes of earlier generations and how information on the internet came back to haunt them. Gen Z'ers recognize the differences between public and private online venues and carefully guard their privacy. They fully expect that marketers will collect data to customize their online experience. While they expect that their preferences are not private, they fully expect that their communications are private. Thus, privacy was also a dominant theme in the response data (in Figures 8 and 9). Figure 10 shows that 6–8th graders immediately considered privacy concerns in their first response.

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. Moreover, about 35% of the younger children reported getting help from family members in remembering their passwords, 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 with friends.

Password management lifecycle

It is necessary to consider users' password behaviors in a holistic manner, realizing that there are three stages in the 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 6–8th graders reported experiencing more difficulties with their passwords. Approximately 20% more of the 6–8th graders than the 3rd to 5th graders reported difficulties in

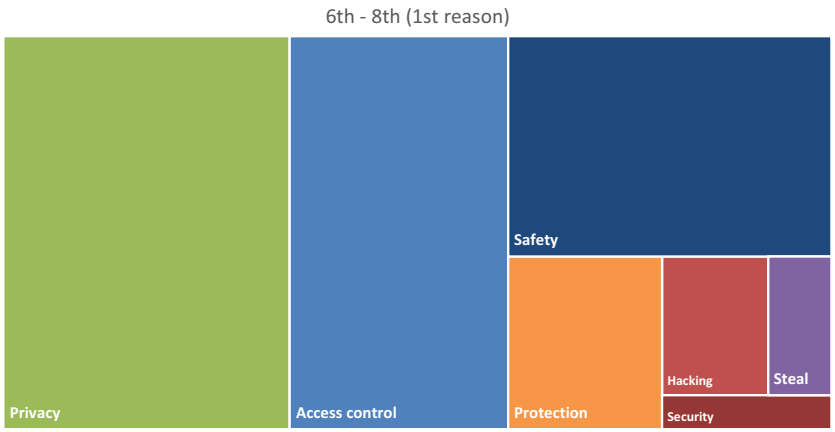

Figure 10: Why passwords? (6–8th)—only looking at the first reason given.

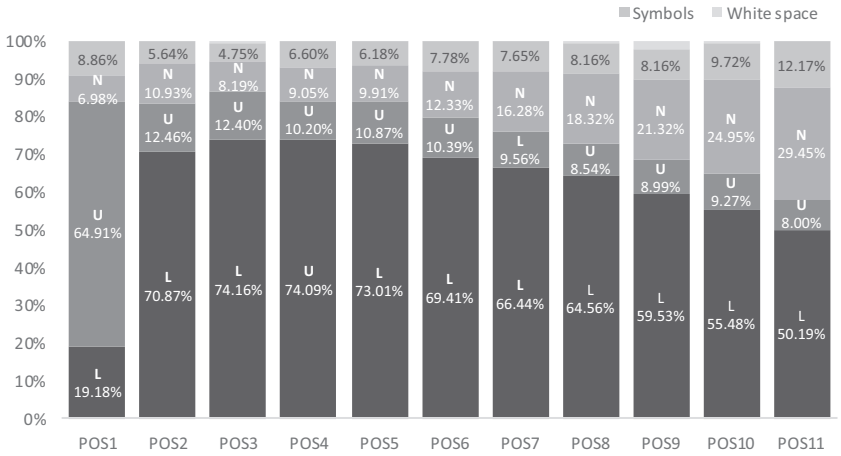

Figure 11: Character types by positions in passwords (by adults).

(L—lowercase, U—uppercase, N—numbers). Adapted from [15]

creating passwords (Table 10). They also struggled more to maintain their passwords: 20% more of the older group reported using "same password for everything" (Table 7), probably because about 12% more of the older children found it difficult to remember passwords (Table 10). 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.

Password choice

On average, the 6–8th graders created passwords that were three characters longer than the 3rd to 5th graders did. Compared to the 6–8th graders, the 3rd to 5th graders used more uppercase letters, numbers, and white spaces when composing their passwords. The 3rd to 5th graders tend to start their passwords with numbers or uppercase letters in the first position. Immediately after the first position, lowercase letters and numbers dominate the next few positions until towards the end of the password where almost two-third of the characters are lowercase letters. The 6–8th 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 first position, the 6–8th 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 [15], the researchers found that uppercase letters dominate the first position in the password, then the rate of uppercase letters sharply drops at the second position, while the lowercase letters substantially rise at position 2, as shown in Figure 11. 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 6–8th graders' password trend (Figure 6) 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 3rd to 5th graders, only eight characters appeared with frequency higher than or equal to 3%, namely, 2, 1, a, e, o, 3, 5, and 6. For the 6–8th 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 3rd to 5th graders. There was some increasing usage of special characters by the 6–8th 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 to 5th graders are:

"12345", "Yellow", "PrincessFrog248", and "doggysafesecure". Some passwords created by the 6–8th 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 six special characters appeared in the passwords created by the 3rd to 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 6–8th 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) [16].

Conclusion

This study finds that children have appropriate mental models of passwords. They understand that passwords provide access controls, protect their privacy, and ensure their stuff's safety. At this point, they are not yet plagued by the overwhelming number of passwords that adults must manage. Children on average reported having 2 passwords for school and 3–4 passwords for home while adults have many passwords, for example, 9 passwords for work [17] and 25 passwords for online accounts [18]. As a result, the children demonstrated good password practices such as memorizing passwords, limiting writing passwords down, keeping their passwords private, and they log out after each session. However, children did not possess the cognitive abilities and extensive vocabulary to form strong passwords. Generating strong passwords requires mature cognitive and linguistic capabilities which children at this developmental stage have not yet mastered.

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 [19]. Our data indicates that children have positive attitudes (in Table 10) and fairly accurate mental models of passwords and authentication. Thus, cyber-security education should strive to reinforce these positive practices while continuing to provide and promote age-appropriate developmental security skills.

This article reports the findings of a case study from two US Midwest schools. A limitation of this case study is that sample only includes 3rd to 8th graders. We have collected over 1500 data points from an additional six US school districts that include 3rd through 12th graders. We plan to perform thorough statistical analysis on the entire dataset to further validate the findings in this paper and increase generalizability.

Conflict of interest statement. Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

References

1. MacFarlane S, Read J, Höysniemi J. *et al*. Half-day tutorial: evaluating interactive products for and with children. *Interact* 2003;1027–1028.
2. Hanna L, Risden K, Alexander K. Guidelines for usability testing with children. *Interactions* 1997;**4**:9–14.
3. Renaud K, Maguire J. Regulating access to adult content (with privacy preservation). In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 4019–4028. Seoul, Republic of Korea: ACM, 2015.
4. Loban W. *The Language of Elementary School Children*. Champaign, IL: National Council of Teachers of English, 1963.
5. Kress G. *Before Writing: Rethinking the Pathway into Writing*. London, UK: Routledge, 1997.
6. Choong Y-Y, Theofanos M, Renaud K *et al*. Case study – exploring children's password knowledge and practices. In: *Proceedings USEC*. San Diego, 2019. https://dx.doi.org/10.14722/usec.2019.23027
7. Renaud K. Web authentication using Mikon images. In: *Privacy, Security, Trust and the Management of e-Business, 2009. Congress'09. World Congress on*. pp. 79–88. Washington, DC: IEEE, 2009.
8. Coggins PE III. Implications of what children know about computer passwords. *Comp Sch* 2013;**30**:282–93.
9. Cole J, Walsh G, Pease Z. Click to enter: Comparing graphical and textual passwords for children. In: *Proceedings of the 2017 Conference on Interaction Design and Children*, IDC '17. pp. 472–77, ACM, 2017.
10. Lamichhane DR, Read JC. Investigating children's passwords using a game-based survey. In: *Proceedings of the 2017 Conference on Interaction Design and Children*, IDC '17. pp. 617–22, New York, NY: ACM, 2017.
11. Coggins PE III. A pedagogical example of second-order arithmetic sequences applied to the construction of computer passwords by upper elementary grade students. *Int J Math Educ Sci Technol* 2015;**46**: 441–450.
12. Berkup SB. Working with generations X and Y in generation Z period: management of different generations in business life. *Mediter J Soc Sci* 2014;**5**:218.
13. 7 Unique Characteristics of Generation Z. (January 25, 2018). *Oxford Royale Academy*. Retrieved from https://www.oxford-royale.co.uk/articles/7-unique-characteristics-generation-z.html
14. Choong Y-Y. A cognitive-behavioral framework of user password management lifecycle. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. pp. 127–37. Heraklion, Crete, Greece: Springer, 2014.
15. Lee PY, Choong Y-Y. Human generated passwords–the impacts of password requirements and presentation styles. In: *International Conference*

on Human Aspects of Information Security, Privacy, and Trust. pp. 83–94. Los Angeles, CA, USA: Springer, 2015.
16. Grassi PA, Newton EM, Periner RA. *et al*. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Technical Report 800-63B, NIST Special Publication, 2017.
17. Choong Y-Y, Theofanos M, Liu H-K. *United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study*. NISTIR 7991, 2014.
18. Florêncio D. Herley C. A large-scale study of web password habits. In: *Proceedings of the 16th International Conference on World Wide Web*. pp. 657–66. Banff, Alberta, Canada: ACM, 2007.
19. Choong YY, Theofanos M. What 4, 500+ people can tell you–employees' attitudes toward organizational password policy do matter. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. pp. 299–310. Cham: Springer, 2015.

Appendix: Surveys

For 3rd to 5th graders:

OMB Number: 0693-0043 | Expiration Date: 12/31/2018

Survey on Youth Password Practices Grades 3 to 5

1. **What types of computers do you use at school and at home?**
   - a. **Desktop computers** ① Yes ② No
   - b. **Laptop computers** ① Yes ② No
   - c. **Tablets (for example, iPad)** ① Yes ② No
   - d. **Cell phones** ① Yes ② No
   - e. **Gaming systems (for example, PS4, Xbox, Wii)** ① Yes ② No
   - f. **Are there other types of computers that you use? If yes, write them down:**

2. **Where do you use computers?**
   - a. **At school** ① Yes ② No
   - b. **At after-school program** ① Yes ② No
   - c. **At home** ① Yes ② No
   - d. **At relative's house (for example, grandparents)** ① Yes ② No
   - e. **At public library** ① Yes ② No
   - f. **Are there other places? If yes, write them down:**

3. **When are you allowed to have screen time with computers, Monday through Friday?**
   - ① Before school
   - ② After school
   - ③ Before bedtime
   - ④ No screen time is allowed during the week

4. **When are you allowed to have screen time with computers, Saturday or Sunday?**
   - ① Only on Saturday
   - ② Only on Sunday
   - ③ Both Saturday and Sunday
   - ④ No screen time is allowed during the weekend

5. **What do you do on computers?**
   - a. **School work** ① Yes ② No
   - b. **Homework** ① Yes ② No
   - c. **Games** ① Yes ② No
   - d. **Use internet** ① Yes ② No
   - e. **Entertainment (for example, YouTube, Nickelodeon)** ① Yes ② No
   - f. **Email** ① Yes ② No
   - g. **Texting** ① Yes ② No
   - h. **Social media (for example, Facebook, Twitter, Snapchat, Instagram)** ① Yes ② No
   - i. **Are there other things that you do on computers? If yes, write them down:**

6. **How many passwords do you have for school?** ① I don't know
   - a. **How many passwords do you have at home?** ① I don't know

1

Survey on Youth Password Practices: Grades 3 to 5 OMB Number: 0693-0043 | Expiration Date: 12/31/2018

7. I use passwords to unlock:
   a. School computers
      ① Yes ② No ③ I don't use a school computer.
   b. Home computers
      ① Yes ② No ③ I don't have a home computer.
   c. Tablets (for example, iPad)
      ① Yes ② No ③ I don't have a tablet.
   d. Cell phones
      ① Yes ② No ③ I don't have a cell phone.
   e. Games
      ① Yes ② No ③ I don't play games.
   f. Email
      ① Yes ② No ③ I don't use email.
   g. Social media (for example, Facebook, Twitter, Snapchat, Instagram)
      ① Yes ② No ③ I don't use social media.
   h. Are there other times when you use a password?
      If yes, write them down:

8. About how many times a day do you use your passwords?

9. How do you get your passwords?
   a. I am given a password by school.
      ① Yes ② No
   b. I make my own passwords by myself.
      ① Yes ② No
   c. My parent/guardian makes passwords for me.
      ① Yes ② No
   d. I make my passwords with help from my parent/guardian.
      ① Yes ② No
   e. Are there any other ways you make a password?
      If yes, write them down:

10. How do you remember your passwords?
   a. I remember the passwords.
      ① Always ② Sometimes ③ Never
   b. I let the computer save the passwords.
      ① Always ② Sometimes ③ Never
   c. I write my passwords down on paper.
      ① Always ② Sometimes ③ Never
   d. A family member remembers my passwords for me.
      ① Always ② Sometimes ③ Never
   e. A friend remembers my passwords for me.
      ① Always ② Sometimes ③ Never
   f. I save my passwords in a file on a computer.
      ① Yes ② No
   g. Are there any other ways that you remember your passwords?
      If yes, write them down:

11. Where did you learn about good password use?
   a. At school
      ① Yes ② No
   b. At home
      ① Yes ② No
   c. On internet
      ① Yes ② No
   d. From friends
      ① Yes ② No
   e. Are there other places you learned about good password use?
      If yes, write them down:

2

Survey on Youth Password Practices: Grades 3 to 5 OMB Number: 0693-0043 | Expiration Date: 12/31/2018

12. Let's talk about your passwords:

a. Do you share your passwords with friends?
① Always ② Sometimes ③ Never

b. Do you use the same password for everything?
① Always ② Sometimes ③ Never

c. Do you keep your passwords private?
① Always ② Sometimes ③ Never

d. When you finish with computers do you sign out?
① Always ② Sometimes ③ Never

e. Do you change your passwords?
① Always ② Sometimes ③ Never

→ **If you selected "Always" or "Sometimes," when do you change your passwords?**

e1. When the computer tells me to
① Yes ② No

e2. When the school tells me to
① Yes ② No

e3. When my family tells me to
① Yes ② No

e4. When I forget my passwords
① Yes ② No

e5. When someone finds out my passwords
① Yes ② No

e6. Are there other times you change your passwords? If yes, write them down:

13. What do you think about passwords?

a. It is easy to make my passwords.
① Yes ② No ③ I don't make my passwords.

b. It is easy to make many different passwords.
① Yes ② No ③ I don't make my passwords.

c. It is easy to remember my passwords.
① Yes ② No ③ I don't know.

d. It is easy to enter my passwords with a keyboard.
① Yes ② No ③ I don't know.

e. It is easy to enter my passwords on a touch screen.
① Yes ② No ③ I don't know.

f. I wish there was another way to unlock besides passwords.
① Yes ② No ③ I don't know.

g. I have too many passwords.
① Yes ② No ③ I don't know.

14. Why do you think people should use passwords?

15. 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.)*

3

Survey on Youth Password Practices: Grades 3 to 5 OMB Number: 0693-0043 | Expiration Date: 12/31/2018

DEMOGRAPHICS

1. **Are you a:**
   - (1) Boy
   - (2) Girl
   - (3) Other
   - (4) Prefer not to answer

2. **How old are you?**

3. **What grade are you in?**

4. **What is your school's name?**

5. **What city do you live in?**

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 30 minutes, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Mary Theofanos, maryt@nist.gov, (301) 975-5889.

4

For 6–12th graders:

OMB Number: 0693-0043 | Expiration Date: 12/31/2018

Survey on Youth Password Practices Grades 6 to 12

1. **What types of computers do you use?** (Bubble in all that apply.)
   - (1) Desktop computers
   - (2) Laptop computers
   - (3) Tablets (for example, iPad)
   - (4) Cell phones
   - (5) Gaming systems (for example, Xbox, PS4, Wii)
   - (6) Are there any other types of computers that you use? If yes, write them down:

2. **Where do you use computers?** (Bubble in all that apply.)
   - (1) At school
   - (2) At after-school program
   - (3) At home
   - (4) At relative's house (for example, grandparents)
   - (5) At public library
   - (6) Are there other places? If yes, write them down:

3. **About how much time do you spend on computers each day, Monday through Friday (both at school and outside of school)?**
   - (1) I don't go on
   - (2) Less than 1 hour per day
   - (3) 1 to 2 hours per day
   - (4) 3 to 5 hours per day
   - (5) More than 5 hours per day

4. **About how much time do you spend on computers each day, Saturday or Sunday?**
   - (1) I don't go on
   - (2) Less than 1 hour per day
   - (3) 1 to 2 hours per day
   - (4) 3 to 5 hours per day
   - (5) More than 5 hours per day

5. **What do you do on computers?** (Bubble in all that apply.)
   - (1) Schoolwork
   - (2) Homework
   - (3) Games
   - (4) Use internet
   - (5) Entertainment (for example, YouTube)
   - (6) Email
   - (7) Texting
   - (8) Social media (for example, Facebook, Twitter, Snapchat, Instagram)
   - (9) Are there other things that you do on computers? If yes, write them down:

6. **How many passwords do you have for school?**
   - (1) I don't know.

   a. **How many passwords do you have at home?**
   - (1) I don't know.

7. **I use passwords to access:** (Bubble in all that apply.)
   - (1) School computers
   - (2) Home computers
   - (3) Tablets
   - (4) Cell phones
   - (5) Games
   - (6) Email
   - (7) Social media (for example, Facebook, Twitter, Snapchat, Instagram)
   - (8) Are there any other times when you use a password? If yes, write them down:

8. **About how many times a day do you use your passwords?**

9. **How do you get your passwords?** (Bubble in all that apply.)
   - (1) I am given a password by school.
   - (2) I make my own passwords by myself.
   - (3) My parent/guardian makes passwords for me.
   - (4) I make my passwords with help from my parent/guardian.
   - (5) Are there any other ways you make a password? If yes, write them down:

1

Survey on Youth Password Practices: Grades 6 to 12 OMB Number: 0693-0043 | Expiration Date: 12/31/2018

10. How do you remember your passwords? (Bubble in all that apply.)

1. I memorize the passwords.
2. I let the computer save the password and fill it in for me.
3. I write my passwords down on paper.
4. A family member remembers my passwords for me.
5. A friend remembers my passwords for me.
6. I save my passwords in a file on a computer.
7. I save my passwords in special software for passwords only.
8. Are there any other ways that you remember your passwords? If yes, write them down:

11. Do you help your family members with passwords?

1. Yes
2. No

→ **If yes, how?** (Bubble in all that apply.)

1. I help them make their passwords.
2. I help them remember their passwords.
3. Are there any other ways that you help them with passwords? If yes, write them down:

12. Where did you learn about proper use of passwords? (Bubble in all that apply.)

1. At school
2. At home
3. On internet
4. From friends
5. Are there other places you learned about passwords? If yes, write them down:

13. Let's talk about your passwords:

A. Do you share your passwords with friends?

1. Always
2. Sometimes
3. Never

B. Do you use the same password for everything?

1. Always
2. Sometimes
3. Never

C. Do you keep your passwords private?

1. Always
2. Sometimes
3. Never

D. When you finish with computers do you sign out?

1. Always
2. Sometimes
3. Never

E. Do you change your passwords?

1. Always
2. Sometimes
3. Never

→ **If you selected "Always" or "Sometimes," when do you change your passwords?** (Bubble in all that apply.)

1. When the computer prompts me to
2. When the school tells me to
3. When my family tells me to
4. When I forget my passwords
5. When someone finds out my passwords
6. Are there other times you change your password? If yes, write them down:

2

Survey on Youth Password Practices: Grades 6 to 12 OMB Number: 0693-0043 | Expiration Date: 12/31/2018

14. What do you think about passwords?

A. It is easy to make my passwords.
1. Agree
2. Neutral
3. Disagree
4. I don't make my passwords.

B. It is easy to make many different passwords.
1. Agree
2. Neutral
3. Disagree
4. I don't make my passwords.

C. It is easy to remember my passwords.
1. Agree
2. Neutral
3. Disagree

D. It is easy to enter my passwords with a keyboard.
1. Agree
2. Neutral
3. Disagree

E. It is easy to enter my passwords on a touch screen.
1. Agree
2. Neutral
3. Disagree

F. I would prefer another way to unlock besides passwords.
1. Agree
2. Neutral
3. Disagree

G. I have too many passwords.
1. Agree
2. Neutral
3. Disagree

15. Why do you think people should use passwords? List up to 3 reasons:

Reason 1

Reason 2

Reason 3

16. 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.)*

DEMOGRAPHICS

1. Are you a:
1. Boy
2. Girl
3. Other
4. Prefer not to answer

2. How old are you?

3. What grade are you in?

4. What is your school's name?

5. What city do you live in?

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 15 minutes, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Mary Theofanos, maryt@nist.gov, (301) 975-5889

3