‘Passwords Keep Me Safe’ – Understanding What Children Think about Passwords

Mary Theofanos and Yee-Yin Choong, *National Institute of Standards and Technology;* Olivia Murphy, *University of Maryland, College Park*

https://www.usenix.org/conference/usenixsecurity21/presentation/theofanos

This paper is included in the Proceedings of the
30th USENIX Security Symposium.

August 11–13, 2021

978-1-939133-24-3

‘Passwords Keep Me Safe’ – Understanding What Children Think about Passwords

Mary Theofanos, *National Institute of Standards and Technology*
Yee-Yin Choong, *National Institute of Standards and Technology*
Olivia Murphy, *University of Maryland, College Park*

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 the fact that the world’s cyber posture and culture will be dependent on today’s youth, it is imperative to conduct cybersecurity research with children. We conducted the first large-scale survey of 1,505 3rd to 12th graders from schools across the United States. Not surprisingly, children have fewer passwords than adults. We found that children have complicated relationships with passwords: on one hand, their perceptions about passwords and statements about password behavior are appropriate; on the other hand, however, they simultaneously do not tend to make strong passwords, and practice bad password behavior such as sharing passwords with friends. We conclude with a call for cybersecurity education to bridge the gap between students’ password knowledge with their password behavior, while continuing to provide and promote security understandings.

1 Introduction

School children are engaged in technology and cyber learning at very young ages. In fact, today’s primary and secondary school children referred to as “digital natives” [32] or “neo-digital natives” [29] have never experienced a world without technology. Computer technology is just a part of their lives. As a result, children are exposed to more and more systems designed specifically for them as well as accessing and using ubiquitous applications such as social media. Many of these systems require authentication to retain a history of interaction, or to ensure that it is genuinely the child using the system. Without evidence of clearly superior and appropriate alternatives, it is understandable that developers implement passwords. As a result, children are actively and frequently using passwords, making understanding their password practices and behavior important.

Usability testing with children is constrained by strict ethical requirements which may discourage researchers from testing authentication mechanisms with this target group altogether [16, 26]. 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. Without an understanding of extant behavior, it is infeasible to start seeking an alternative, more appropriate, mechanism for child-tailored authentication. Despite extensive studies of password practices of participants over 18 years old (e.g., [1, 7, 14, 17, 31, 43]), children’s password practices have not been well studied.

To understand current children’s password perceptions and behavior, we conducted a study to answer the following research questions (RQ):

RQ1. Password Understandings:
- (a) What do students know about passwords?
- (b) Why do they think they need passwords?
- (c) What are students’ passwords perceptions?

RQ2. Password Behaviors:
- (a) How do students create and maintain passwords?
- (b) What are the characteristics of passwords they create?

The contributions of this paper are threefold:
1) Firstly, we conducted the first large-scale study on the use, perceptions and behavior of passwords of the United States (US) youth 3rd to 12th grades–Generation Z (Gen Z) those born from the mid-1990’s to the late 2000’s [29];
2) Secondly, we characterize the state of children’s perceptions and knowledge of passwords;
3) Finally, we offer concrete suggestions for next steps in both youth password research and education.

We next review related work. We present our methodology followed by results, discussion and conclusions.

2 Related Research

In 2015, 94% of US children between the ages of 3 and 18 had a computer at home, and 86% of children had internet access at home [39]. As of 2019, 53% of children own their own smartphone by age 11, with that number rising to 84% among teenagers [11]. Children around the world are going online more, at younger ages, and in more diverse ways [13]. Children spend more time on screen media performing various activities such as TV/videos, gaming, browsing websites, and social media [11]. As children are doing more activities online, they are creating user accounts and passwords as required by those online systems. However, the research topic on children's password perceptions and practices has not been extensively studied, so there is a comparative lack of literature available.

In 2019, Choong *et al* [9] performed a systematic search on cybersecurity research involving children and classified 78 papers into two major categories – Designing for Children, and Children & Authentication which each was further broken into six sub-categories. They identified a gap in the literature related to children's password comprehension and practices. This present study seeks to fill that gap.

Several researchers performed empirical studies on children's passwords with small numbers of participants, usually with narrow (two years) age ranges (e.g., [21, 27, 33]). These studies agree that the younger a child is the less complex their passwords are and should be required to be due to age-specific factors like memory and spelling, and that children frequently use personal information in password creation [21, 27, 33]. Other researchers used surveys to gather larger amounts of data on children's password knowledge and behaviors and found similar results. For example, Rim and Choi [35] analyzed password generation types from 550 middle and high school students in South Korea and concluded that students are likely to use personal information in their passwords. Further, the study found that participants seldom worried about protecting passwords and personal information. This is concerning because, as revealed in Irwin's [23] investigation of 258 10th to 12th grade South African Students' risk taking behavior and awareness, students in this age group have a high level of risk and gaps in their risk awareness and avoidance behavior. Coggins [10] conducted a small-scale survey on children's password knowledge from 74 4th to 6th grade students that supports all of the above studies, finding that 70% of participating students used personal information in their passwords and 32% had experienced hacking. Our present study seeks to build upon these findings by investigating a full range of school-age students from 3rd to 12th grade, and exploring not only students' password behavior, but also their perceptions and understandings about the role of passwords.

In addition to the field of knowledge surrounding children's password behavior, several studies have investigated children's perceptions of online privacy and security more broadly. For example, Kumar *et al* [24] interviewed 18 US families with children ages 5 to 11, and found that children on the upper end of that age range generally recognized certain privacy and security components, but that younger participants (5-7) had gaps in their knowledge. Zhang-Kennedy *et al* [45] similarly conducted interviews with 14 Canadian parent-child dyads with children ages 7 to 11 to understand their concept of privacy and perceptions of online threats. The study found that children and adults view online privacy and security differently, with children being less concerned than their parents about security threats and mostly worried about threats from local (family, friends, etc.) sources. Our present study seeks to combine the focus on perception in the above studies with an emphasis on password knowledge and understandings as well as password use.

Methodologically speaking, researchers frequently use surveys and questionnaires in order to understand children's perceptions and awareness of online safety, privacy and security. For example, Žufić *et al* [46] administered three surveys over the course of eight years to 1,232 students ages 7 to 15 in Croatia to find that student use of information-telecommunication technology is increasing over time, but student safety awareness is not. Yilmaz *et al* [44] similarly deployed a survey to 2,029 Turkish high school students and revealed that only about half of the students surveyed have high awareness of how to ensure information security toward threats. Paluckaitė *et al* [30] survey of 152 Lithuanian adolescents' perceptions of risky online behavior adds nuance to these security threat understandings by revealing that many participants do understand risky behavior as risky but still engage in them, which may or may not be a product of their awareness of privacy and security threats. Across the board, these studies serve as precedents for our own use of surveys to investigate students' password use, perceptions, and behaviors.

Based on the literature reviewed above, currently existing research often uses a small sample size, does not cover a full age range of K-12 students, and usually does not offer inferential comparisons among kids at different developmental stages in order to gain insight on age-related progression in children's understanding of cybersecurity and privacy. While there have been a few larger-scale survey studies, they have been all focusing on children outside of the US. Investigation in this area to understand and gauge current levels of US children's comprehension and practice related to passwords is essential to provide insights into overall children's cybersecurity hygiene. This study seeks to add to the burgeoning field of scholarship surrounding children's password use, perceptions, and understandings while also addressing the aforementioned shortcomings in the field by conducting a large-scale survey of students between ages 8 and 18 (3rd to 12th grades) in the United States.

3 Method

We developed a large-scale, self-report survey to understand what challenges US grade school children face regarding passwords. The target population was students from 3rd to

12th grades (ages of 8 to 18 years old). 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.

3.1 Survey Development

The research questions guided the development of survey objectives for accessing student's use of computers, of passwords, password practices, knowledge about passwords, feelings about passwords, and tests for age differences. A list of possible items was generated targeting the objectives. All of the items were closed response except for two numerical response and two 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 create a new password for a given scenario.

Early in survey development, feedback from teachers and a pilot survey suggested that two surveys featuring the same questions but using different, age-appropriate language would be required to accommodate the wide age range of the intended student population. Thus, two surveys were designed: a 15-item survey for 3rd to 5th graders, and a 16-item survey for 6th to 12th graders. The extra item in the 6th to 12th grade survey asked students whether they have experience helping their family members with passwords. The content of the other 15 questions was identical across the two surveys, with the language and format of the response variables adjusted to be age appropriate. For example, most of the response variables were "*Yes*" or "*No*" for the 3rd to 5th graders, while the 6th to 12*th* graders' response variables were more detailed and they were asked to check all variables that apply.

To ascertain the content and construct validity of the survey instruments, four types of reviews were conducted iteratively. 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, the alignment of the items with the category, and the possibility of missing items. Survey experts also reviewed each item for clarity for the intended audience, appropriate format, 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. As a pilot, cognitive interviews with students were also conducted using a talk-aloud protocol to determine if the questions were being appropriately interpreted. 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. After each type of review, the survey instruments were refined based on the feedback and comments. The final surveys were converted to Scantron© forms–machine readable paper forms as shown in the Appendix.

3.2 Procedure & Recruitment

The National Institute of Standards and Technology Institutional Review Board reviewed and approved the protocol for this project and all subjects provided informed consent in accordance with 15 CFR 27, the Common Rule for the Protection of Human Subjects. The sampling plan focused on recruiting participants from at least three different school districts from three different US regions–the East, South, and Midwest–in order to collect a geographically diverse and more nationally representative sample population. Principals and teachers from the selected districts were recruited using a snowball sampling approach. The principals were to determine which classrooms would participate, and the selected classroom teachers would distribute parental consent forms.

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 or ear buds, for example. Each participating classroom also received $50 for a classroom thank-you celebration where all students celebrated. Parental consent and student assent forms were collected prior to survey distribution. 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. All open-ended responses were manually entered into a spreadsheet by the researchers. Each completed survey was assigned a unique random participant identifier, for example, P1234.

3.3 Participants

A total of 1,505 3rd to 12th grade students from schools across the South, Midwest, and Eastern regions in the United States completed the survey. Demographics are shown in Table 1.

Students	#	**Gender** (%)			**Age** (Years)	
		Boy	Girl	Others[1]	Mean	SD
ES	425	40.2	51.9	7.9	9.03	0.92
MS	357	45.1	50.3	4.6	12.46	1.01
HS	723	44.7	51.4	3.9	15.79	1.21

Table 1. Participant Demographics

[1] This includes "other" and "prefer not to answer" responses.

Participants included 425 3rd to 5th grade elementary school students (ES) from four elementary schools, 357 6th to 8th grade middle-school students (MS) from four middle schools, and 723 9th to 12th grade high school students (HS) from three high schools.

3.4 Data Analysis Procedure

Descriptive statistics were used to report the frequency and percentage of the categories that participants chose as responses to the multiple-choice questions. We compared groups using inferential statistics with an overall significance level set at $\alpha = 0.05$.

For categorical variables, Chi-Square tests of association were used, with effect size calculated using Cramer's V. For measured variables with interval levels, data were first tested for normality. Nonparametric tests (Mann-Whitney U test to compare two groups) were applied as the data were not normally distributed. P*ost-hoc* comparisons were used to compare groups: ES vs. MS, MS vs. HS, and ES vs. HS while applying the Holm-Bonferroni method to control the family-wise error rate [19] with adjusted $\alpha = 0.017$.

Qualitative responses to the open-ended question "*Why do you think people should use passwords?*" were coded using a two-cycle coding process [36]. In the first cycle, inductive thematic and in vivo coding were used separately by two members of the research team, and then discussed and merged into one set of codes and sub-codes. We calculated intercoder reliability for the initial coding of the data using the ReCal2[2] software, the Krippendorf's Alpha score was 0.968. Second cycle pattern coding was used to condense the larger code deck into major themes, and returned three final thematic codes–access, privacy, and safety–that were applied to all of the data [36]. A third, qualitatively trained researcher was then brought in to independently conduct the same inductive two-cycle coding process to further validate results, and to advise on qualitative thematic consolidation and discussion. The third coder returned four themes: safety, privacy, offensive and defensive access, and protection. The new theme "protection" was discussed by the research team and also applied to the data.

The third researcher also performed a single-cycle deductive thematic coding of the responses to the second open-response survey question asking participants to create a password. The themes for the deductive coding–perceived personal information, number or word-only, alphanumeric, and strong/weak–were derived from the afore cited literature in order to check the validity of collected data with currently existing theories and research surrounding children's password creation behavior.

Any quotes provided within this paper as exemplars are verbatim from the children's responses. The quotes are presented in italics and followed by a notation with the unique participant identifier and the participant's grade. For example, (P745, 3rd) indicates a quote from P745 who was a 3rd grade student.

4 Results

As indicated in section 3.4, the significance level of statistical analyses was set at $\alpha = 0.05$ and adjusted $\alpha = 0.017$. The asterisk symbol "*" is used to indicate statistical significance ($p < \alpha$).

4.1 Current Usage

To understand our participants' current usage of computing devices, we collected data on the types of devices as well as activities performed with those devices. The percentages of computing device usage are summarized in Table 2. When comparing among ES, MS, and HS, the MS reported using laptop the least, followed by ES, then HS ($\chi^2 = 43.83$, df = 2). The use of tablets decreases significantly from ES to MS, to HS ($\chi^2 = 46.17$, df = 2), whereas cell phone usage increases significantly from ES to MS, to HS ($\chi^2 = 180.65$, df = 2).

Grade	Desktop (%)	Laptop* (%)	Tablet* (%)	Cell phone* (%)	Gaming console (%)
ES	74.57	84.07	71.86	63.22	68.86
MS	63.28	74.01	53.95	84.75	66.38
HS	61.91	89.20	46.68	91.41	55.68

Table 2. "*What types of computers do you use at school and at home?*"

Students use computers for many activities such as schoolwork, homework, games, texting, and social media (Table 3).

Response Option	ES (%)	MS (%)	HS (%)
Email*	28.15	25.71	57.62
Entertainment	87.90	81.92	82.27
Games*	92.95	77.12	63.85
Homework*	59.59	59.60	86.98
Internet	84.58	73.45	82.69
School	83.50	71.47	87.95
Social media*	38.22	57.91	71.88
Texting*	46.30	55.08	70.36

Table 3. "*What do you do on computers?*"

HS significantly do more homework compared to ES ($\chi^2 = 151.99$, df = 1) and compared to MS ($\chi^2 = 106.22$, df = 1). HS also use emails significantly more than ES ($\chi^2 = 116.40$, df = 1) and more than MS ($\chi^2 = 98.55$, df = 1). When comparing

[2] http://dfreelon.org/utils/recalfront/recal2/

among ES, MS, and HS, social media use increases significantly from ES to MS, to HS ($\chi^2 = 153.79$, df = 2). Likewise, texting increases significantly from ES to MS, to HS ($\chi^2 = 95.83$, df = 2). Finally, playing games decreases significantly from ES to MS, to HS ($\chi^2 = 75.14$, df = 2).

4.2 Password Understandings

Students reported learning about good password practice mainly from home (72.35%) and school (59.90%) as opposed to learning from internet (24.48%) and friends (12.28%).

4.2.1 Why Passwords?

Students were asked "*Why do you think people should use passwords?*" ES were asked to provide one reason while MS and HS were asked to provide up to three reasons.

As mentioned previously, the responses were coded using a two-cycle thematic process. There were 7 primary codes/sub-codes and 20 in vivo operationalization terms for those codes, such as "security." The final code book of primary codes, sub-codes, and in vivo terms is shown in Table 4.

Primary Code	Sub-code	Code Operationalization
Access		Mentioned the ability (i.e., allow access) or inability (i.e., prevent access) to use accounts, devices, data, information
	Hacking	Mentioned *hack* or *hacking* (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)

Table 4. Why Passwords – Qualitative Analysis Code Book

The percentages of responses in each primary and sub-code are shown in Table 5. As shown in Table 5, for ES, *Access* was the most frequently provided reason for passwords for ES, followed by *Safety*. The ES' responses included both preventing access and providing access. Response examples were "*To keep people out of their stuff*" (P745, 3rd) and "*They should use it because the computer needs to know who they are"* (P623, 5th). Representative examples for *Safety* included "*To keep us safe*" (P1131, 4th), "*To keep their stuff safe*" (P722, 5th) and "*... because someone might track you down*" (P691, 3rd). Almost all MS cited *Access*, but *Privacy* was the second most common response. Exemplar MS' responses include *Access*: "*To lock up everything"(*P2652, 7th) and "*So people don't login and be nos[e]y*" (P1665, 8th); *Privacy*: "*To keep their information private*" (P2909, 6th) and "*To keep stuff private*" (P2918, 8th). HS were focused on *Privacy* followed by *Access*. Representative HS' responses include: *Privacy*: "*Keep things private*" (P1768, 10th) and "*To keep privacy*" (P2596, 12th); *Access*: "*So no one will get in your stuff"(*P2007, 9th) and "*To keep unwanted people off your device*" (P1392, 11th).

Primary Code	Sub-code	**ES** (%)	**MS** (%)	**HS** (%)
Access		43.04	100.58[3]	61.52
	Hacking	11.14	19.31	11.38
Privacy		19.49	52.16	71.07
Protection		2.78	22.48	31.32
Safety		26.84	39.19	34.27
	Security	0.76	8.65	27.95
	Steal	3.54	12.68	5.62

Table 5. Children's Responses to Why We Need Passwords

Protection, *Security*, *Hacking*, and *Steal* are the remaining codes/sub-codes. *Protection* was cited more frequently by HS and MS than ES. Examples include: "*To be protected*" (P2893, 6th) and "*To protect information*" (P2719, 12th). *Security* was reported more by HS than MS and ES. Example responses include: "*Security reasons*" (P244, 9th) or "*Keep info secure"* (P1319, 12th). *Hacking* was mentioned more frequently by MS, for example, "*to make it harder to get hacked*" (P1433, 6th). *Steal* received the fewest responses across all three age groups (13 % and below). 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* coded data.

[3] Note: a single student's responses can be coded to multiple sub-codes that belong to the same primary code which may result in percentages over 100 %, for example, *Access* for MS.

4.2.2 Password-Related Perceptions

In general, over 50% of the students found it easy to make a password, but less than 50 % found it easy to make many different passwords (Figure 1).

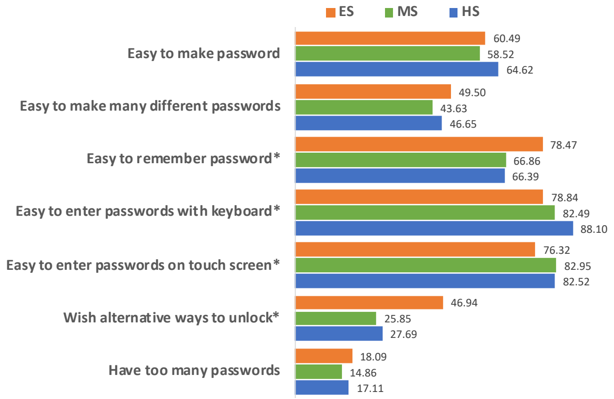


Figure 1. Children's Perception of Passwords (in %)

ES found it significantly easier to remember passwords, compared to MS ($\chi^2 = 6.74$, df = 1) and compared to HS ($\chi^2 = 9.60$, df = 1). While generally students reported it easy to enter passwords (more than 75%) with keyboard or on touch screen, there were significant differences when comparing ES to their older counterparts. Entering password with keyboard becomes significantly easier from ES, to MS, then to HS ($\chi^2 = 32.33$, df = 2). ES found it significantly more difficult to enter passwords on touch screens compared to MS ($\chi^2 = 11.75$, df = 1) and HS ($\chi^2 = 16.47$, df = 1). Finally, significantly more ES wanted alternative ways (other than passwords) to authenticate compared to MS ($\chi^2 = 32.56$, df = 1) and to HS ($\chi^2 = 37.77$, df = 1). Across all three age groups, less than 20 % reported having too many passwords.

4.3 Password Behaviors

4.3.1 Password Habits

Children's password habits are summarized in Table 6.

Response Option	ES (%)	MS (%)	HS (%)
Change passwords*	61.08	78.06	74.13
Keep passwords private*	92.96	97.71	98.46
Share passwords with friends*	22.66	39.49	44.71
Sign out after use	92.07	96.57	92.29
Use the same password for everything*	57.82	80.63	87.29

Table 6. Children's Password Habits

While more than 92% of each group reported that they keep their passwords private, ES reported significantly lower percentage compared to MS ($\chi^2 = 18.18$, df = 1) and to HS ($\chi^2 = 47.21$, df = 1). However, as children age from ES to MS, to HS, they progressively reported significantly more and more that they "share passwords with friends" ($\chi^2 = 60.68$, df = 2). The use of same password for everything also increases significantly from ES, to MS, to HS ($\chi^2 = 149.02$, df = 2). ES reported "change passwords" significantly less often compared to MS ($\chi^2 = 29.59$, df = 1) and to HS ($\chi^2 = 29.06$, df = 1). The two primary reasons (over 60 %) for changing passwords are "*when I forgot my passwords*" and "*when someone finds out my passwords.*" All age groups reported a very high rate (more than 92%) of signing out after use.

4.3.2 Password Selection & Storage

When asked how they get their passwords, all are given passwords by their schools at very high rates as over 80% as summarized in Table 7.

Response Option	ES (%)	MS (%)	HS (%)
Given by School	88.83	82.39	87.79
Make my own passwords*	54.50	81.53	95.28
Made by parents*	45.69	19.60	7.07
Made my own with parents' help*	44.25	17.90	8.32

Table 7. "*How do you get your passwords?*"

As shown in Table 7, younger students (ES) reported having significantly more parental involvement in creating their passwords. Students having passwords made by parents decrease significantly from ES to MS, to HS ($\chi^2 = 209.07$, df = 2). Similarly, students making their own passwords with parents' help decrease significantly from ES to MS, to HS ($\chi^2 = 179.13$, df = 2). And, students making their own passwords increase significantly from ES to MS, to HS ($\chi^2 = 311.09$, df = 2).

Figure 2 shows how students remember passwords. More than 89 % of participants across age groups reported memorizing their passwords as a strategy for remembering passwords.

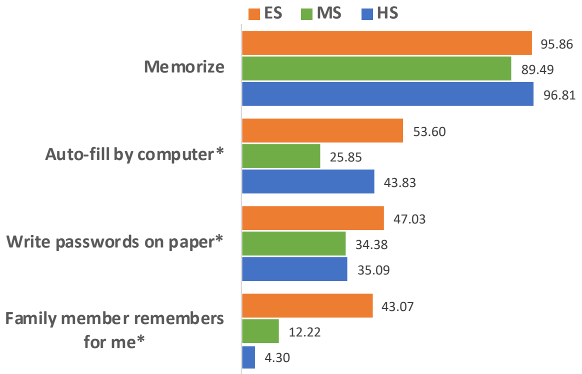


Figure 2. "*How do you remember your passwords?*" (in %)

Approximately half of ES reported that they write their passwords on paper which was significantly higher than MS ($\chi^2 = 9.47$, df = 1) and HS ($\chi^2 = 10.66$, df = 1). The MS reported using auto-fill feature less frequently compared to

ES ($\chi^2 = 52.22$, df = 1) and compared to HS ($\chi^2 = 33.77$, df = 1). As children age, their relying on family members to remember their passwords significantly decreases from ES to MS, to HS ($\chi^2 = 267.96$, df = 2).

Both MS and HS were asked an additional question on whether they help their family members with passwords. About 47 % of MS and 34 % of HS chose "*Yes*." Of those who chose "*Yes*," the primary assistance they provided was to "*Help family members remember passwords*"–MS (68.86 %) and HS (78.01 %).

4.3.3 Created Password Analysis

The three groups were asked to create a password: "*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

On average, students created passwords about 10 characters long (ES: 9.90 characters, MS: 10.42 characters, and HS: 10.44 characters). Using the *Mann-Whitney U* test , ES was found creating significantly shorter passwords, compared to MS ($z = -3.23$) and HS ($z = -4.75$).

Figure 3 shows the distribution of different character types used in the passwords created by the participants. Lowercase letters make up the majority of the passwords, followed by numbers. ES used significantly fewer lowercase letters, compared to MS ($z = -3.44$) and HS ($z = -5.42$). ES used significantly more numbers than MS ($z = 2.52$) and HS ($z = 2.40$). Across all age groups, symbols or white spaces were rarely used.

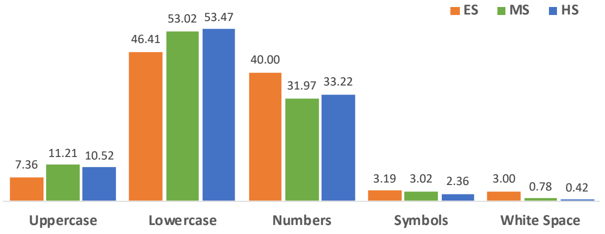


Figure 3. Character Types in Passwords (in %)

We further examined character type positioning in the passwords. Figures 4, 5, and 6 display the overall character type distributions relative to their positions in the passwords, for password lengths of 9 (median) for ES, and password lengths of 10 (median) for MS and HS.

As shown in Figure 4, ES predominantly used lowercase letters and numbers. They tend to start their passwords with numbers or uppercase letters in the 1st position. Immediately after the 1st position, the remaining positions, lowercase letters were used predominantly (about 50 %) and numbers were used between 39 % and 46 %.

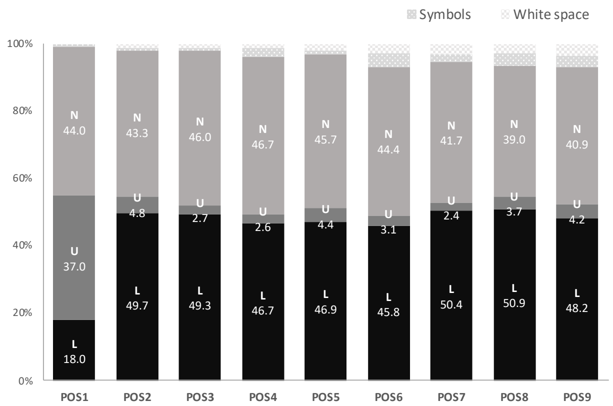


Figure 4. Character Types by Positions in Passwords (ES)

(in %; L – lowercase, U – uppercase, N – numbers)

In contrast, the patterns for MS (Figure 5) and HS (Figure 6) look quite different from ES. Both MS and HS also tend to start their passwords with uppercase letters (about 55%), but numbers are not as prevalent in the first position as for ES. We observe a decreasing use of lowercase and increasing trend of using numbers as the position gets higher.

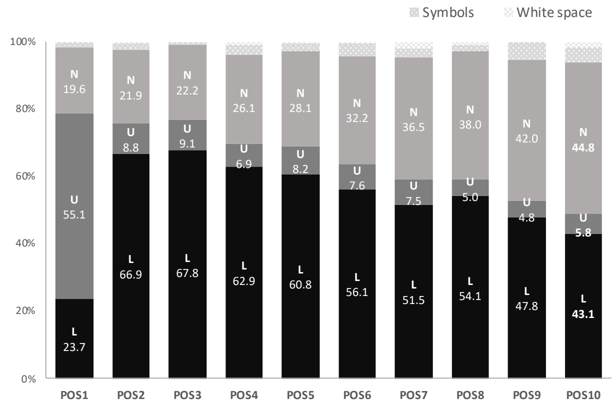


Figure 5. Character Types by Positions in Passwords (MS)

(in %; L – lowercase, U – uppercase, N – numbers)

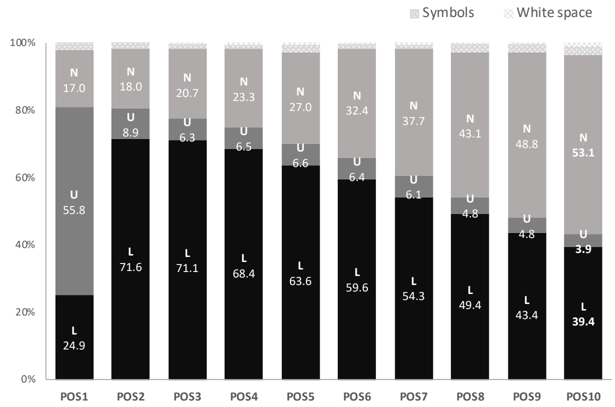


Figure 6. Character Types by Positions in Passwords (HS)

(in %; L – lowercase, U – uppercase, N – numbers)

In addition, the passwords did not use a broad range of characters, much like adults [22]. For all three age groups, only 8 alphabetic characters and four numbers "0, 1, 2, 3" were used with frequency higher than or equal to 3 %.

Many of the passwords contained passphrases or multiple common words. We specifically examined the passwords for the following three characteristics (Table 8):

- *Dictionary word*: a single dictionary word,
- *Dictionary word plus*: a single dictionary word plus numbers and special characters preceding or following the word,
- *Numbers only*: passwords contain all numbers.

Password Characteristics	ES (%)	MS (%)	HS (%)
Dictionary word	4.29	1.25	2.56
Dictionary word plus*	8.85	17.76	15.81
Numbers only*	31.64	13.08	8.12
(All other passwords)	55.22	67.91	73.51

Table 8. Passwords containing dictionary words or numbers

As in Table 8, only a small percentage (under 5 %) of all age groups) created passwords with a single dictionary word. There were significantly fewer ES created passwords using a single dictionary word plus numbers and special characters preceding or following the word– *Dictionary word plus*, as compared to their older counterparts–MS ($\chi^2 = 12.13$, df = 1) and HS ($\chi^2 = 10.19$, df = 1). There were significantly more ES (almost 1/3) created passwords with only numbers, as compared to MS ($\chi^2 = 33.47$, df = 1) and to HS ($\chi^2 = 98.83$, df = 1). In addition, significantly more MS created numbers-only passwords as compared to HS ($\chi^2 = 6.21$, df = 1). This indicates that as children progress from ES to HS, they created fewer and fewer numbers-only passwords.

The created passwords often consist of concepts reflecting the current state of the children's lives. Password themes included references to sports, video games, names, animals, movies, titles (princess, queen, etc.), numbers and colors. Passwords demonstrating these themes by ES include: "*12345*", "*Yellow*", "*doggysafesecure*", and "*PrincessFrog248*". Passwords created by MS include: "*Basketball1130*", "*GameGuy007*", and "*Gamehead77*". Passwords created by HS include: "*callofdutyblackops*", "*ILoveFortnite*", and "*Soccer player.15*". Several children provided their password creation strategies, instead of actually creating an example password. For instance, an ES wrote "*Maybe a birthdate or something.*" (P1168, 4th), another MS wrote "*My gamer tag, then random numbers*" (P2970, 8th), and an HS provided "*firstnamelastname123*" (P2837, 11th).

Password Strength

For the purpose of our study, we measured password strength with the password strength meter which uses the zxcvbn.js[4] 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 rating score provided by zxcvbn.js measures password strength on an ordinal scale with "0" being assigned to a password 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 1,100 and the estimated number of guesses for another password is 9,900, 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 passwords across the three groups.

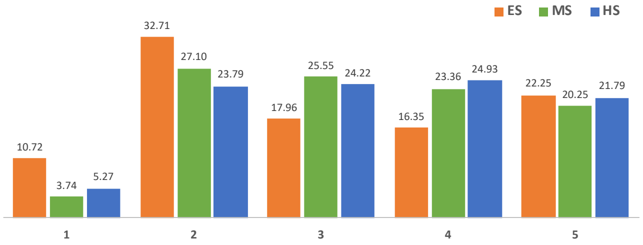


Figure 7. Password Strengths (in %)

The HS' passwords were significantly stronger than the ES' (z = 3.40). The MS' passwords were also significantly stronger (z = 2.42) than the ES'. For those passwords with a score of 1, the students used all numbers or simple common words as proposed passwords such as: "*1206*", "*112233*", "*Yellow*" and "*Game1234*". Examples of strong passwords (those with a score of 5) were:

- by ES: "*Love_Butter56*" and "*Dolphins blue tale*";
- by MS: "*ArrowTurner_8435!*" and "*dancingdinosaursavrwhoop164*";
- by HS: "*Soccer player.15*" and "*Aiken_bacon@28*".

5 Discussion

Not surprisingly, as children age, their use of technology and online activities change. The percentages of students having

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

cell phones increased almost 20 % from ES to MS and another 10 % from MS to HS. With age, social activities naturally increase as described in the PEW article of Teen, Social Media and Technology Study 2018 [2]. Our data confirm this trend—both texting and social media use increase significantly from ES to MS to HS. HS also use email significantly more than ES or MS. The increased technology use translates to needs for authentication for older children. A coping strategy may be that over 80 % of HS and MS reported using the same password for everything much like password reuse of adults [37, 42].

5.1 RQ1: Password Understandings

Generation Z, or those born from the mid-1990's to the late 2000's (the population of focus in this study) have several unique generational characteristics that influence their behavior [3] [29]. For example, they are digital natives and have grown up in a fully digital world where interaction with technologies is a part of normal life, requires authentication, and frequently involves personal information [29]. Additionally, more children are gaining access to a variety of technologies earlier and more frequently than their older counterparts, all of which are reflected in our participants' password understandings.

Participants frequently specifically mentioned securing their personal phones and computers, and were particularly concerned about access: the code *access* was applied to 601 participant responses, and pertained to both personal access to one's own devices/information and preventing unwanted access by others as seen in Figures 8, 9, and 10. For example, (P1880, 6th) indicated that one "*should have a password so that people won't go through your phone*" and (P394, 4th) found passwords to be important "*to unlock games (and) unlock computers*."

Frequently, *access* was associated with matters of *privacy*, as indicated in Figures 9 and 10 which demonstrate that MS and HS participants noted privacy concerns as their primary response. Whereas adults frequently worry about hackers' access to tangible things like bank account information, students frequently use technology for purposes deeply related to their identities like social media, gaming identities, and texting, and their password understandings reflect these uses. In terms of social development, as children–particularly preteens and teenagers like the majority of this study's participants–begin to explore and exercise autonomy, their privacy becomes an increasing concern. In this study, participants frequently emphasized the importance of passwords for personal information privacy, like (P2034, 11th) who commented that passwords "*secure...account(s) on social medi*a" and (P2972, 8th) who commented that passwords make it to where "*your siblings or family/friends can't get to any of your stuff*." Additionally, younger (ES) participants' privacy concerns were more general, whereas their MS and HS counterparts were increasingly more specific to things like gaming, social media, and cell phones. This makes sense, as younger students less frequently have unsupervised access to these applications and therefore do not associate them with expectations of privacy.

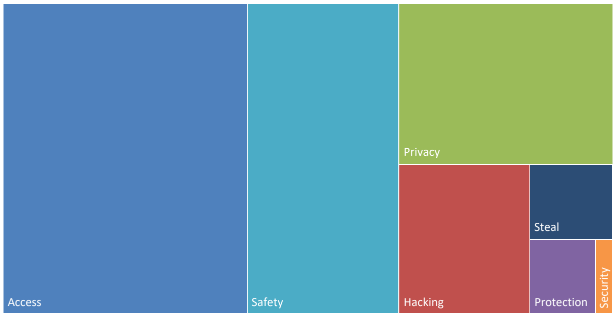


Figure 8. Why passwords? (ES)

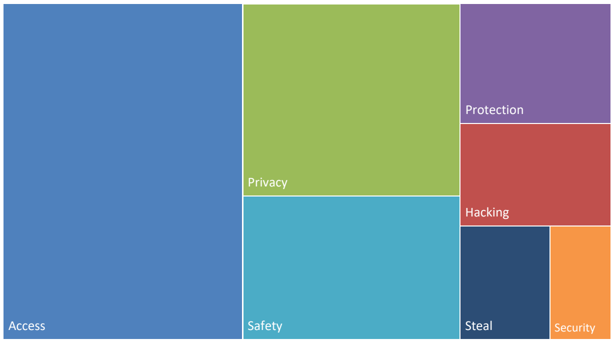


Figure 9. Why passwords? (MS)

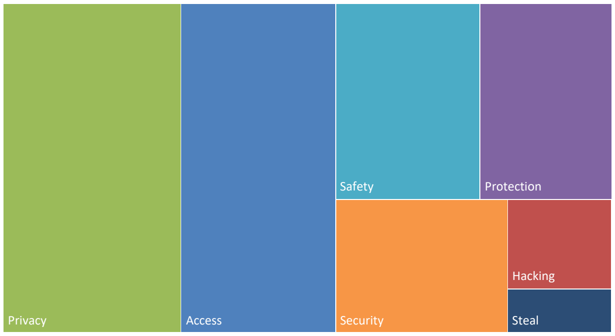


Figure 10. Why passwords? (HS)

Finally, though the idea of safety was an incredibly popular response in the open-ended question about students' password understandings (the words "safe" or "safety" appeared in 609 individual responses) the mentions of safety were, more than any other coded response, vague. For example, the words "safe" or "safety" were most likely to be written alone or accompanied by vague concepts like "things" and "stuff", e.g., "*to keep stuff safe*" (P1396, 11th) and "*to keep things safe*" (P1454, 7th). This raises questions about how much students really know about online/cybersecurity safety and privacy, and how much they have been raised in a digital age that teaches them that passwords and other security measures are important for safety, without ever explaining what that safety means. More open-ended qualitative investigation is needed to understand.

5.2 RQ2: 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 six times as many ES (about 90 %) reported having parental help in creating their passwords, in contrast to HS (about 15 %). Moreover, about 43 % of the younger children reported getting help from family members in remembering their passwords, as compared to only 7 % of the HS.

Both school and parents play an important role of providing guidance on 'good' password hygiene across all age groups. Additionally, almost half of MS and a third of HS reported assisting their family members with remembering passwords.

The participants reported having some good password behaviors including memorizing passwords, limiting writing passwords on paper, keeping their passwords private, and signing out after computer use (as shown in Figure 2 and Table 6). However, students in our study frequently used words (presumably) containing personal information, which is a less secure behavior that is also reflected in other studies of children's password behavior [10, 35]. Additionally, as students grew older, they were increasingly more likely to share their password(s) with friends. In the age of modern technology where at least 84% of teenagers own cell phones [11], this actually makes sense: the use of various in-phone applications, video, and camera functions is ubiquitous and socially casual. Some students share their phone passwords with close friends or significant others in order to establish trust and make access to certain phone functions faster and easier. Unfortunately, this behavior often stands in direct contradiction to the students' own perceptions that sharing passwords is bad.

The simplistic nature of passwords is expected for younger students where literacy is improving as they age. This is especially true with younger students who are working on mastering their alphabet and numbers. Special character use was very scarce across all of the grades. This is evidenced by the fact that very few special characters appeared in the passwords created by the children in this study. The overall use of special characters by ES was less than 0.75 % except for white space which had a frequency of 3.00 %. The few special characters used were common punctuation marks such as comma (,), period (.), dash (-), and exclamation (!).

Despite the awareness shown when discussing the purposes of passwords, the passwords chosen by the children (particularly by the younger age group) were weak. There were improvements in the older groups (both MS and HS are significantly stronger than ES). The MS and HS passwords are equally distributed among scores 2, 3, 4, 5 (Figure 7). Unfortunately, adults also create passwords that are weak and easy to guess [4, 12, 18, 28, 40, 41]. Generally, adults find it difficult to choose passwords that are easy to remember and hard to guess [43] especially given the overwhelming number of passwords they must manage [8, 14]. We did not ask students to explain why they chose the numbers, letters, and characters in their fabricated passwords.

There is clearly a need to address how children, particularly in the younger age group, understand and use passwords in regard to understanding threats to passwords and valuing accounts [38]. Children should be guided in discussions about password strength requirements and why these requirements exist. 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) state that password complexity requirements do not ensure strong passwords; instead, longer passphrase-like passwords are encouraged [15]. It will be helpful to provide guidance to youth on how to evaluate what it is that is being protected, how strong a password is needed, and how to create an appropriate password.

In addition, given the high level of password reuse of HS, it is also important to teach students of the risks of reuse and emphasize that having unique passwords is a more secure approach.

6 Limitations

Our study has several limitations which may limit the generalizability of our findings. First, our sample was a convenience sample based on geography and personal connections with schools. Future studies may use alternative participant recruitment in an effort to minimize potential bias. Second, the hypothetical password creation task can be viewed as contrived. However, it still provides invaluable insight on children's character choices and composition patterns in passwords. The final limitation is the use of self-report data. The youth respondents may have rationalized their behaviors by providing socially desirable explanations. Due to the study format–survey with brief short response questions–we weren't able to ask follow-up questions or ask students to elaborate on their responses or password creation choices. Future studies could use mixed method techniques, such as including interviews, to probe deeper into youths' perceptions on online security and privacy.

7 Conclusion

This study finds that children are not yet plagued by the overwhelming number of passwords that adults must manage. Children on average reported having two passwords for school and two to four passwords for home, while adults report having up to five times that amount [8, 14].

Reinforcing positive perceptions and practices

It is important to promote positive user perceptions about passwords early on [8], and our data indicates that children have reasonably accurate perceptions and knowledge of passwords and authentication. Thus, cybersecurity education should strive to reinforce these positive perceptions while continuing provide and promote security understandings.

Promoting concrete understanding

Our study also reveals that students frequently discuss the significance of passwords very generally and vaguely, often using one or two words like "information" and "safe," and do not put their password knowledge into practice. This raises questions about whether or not students actually understand why certain password practices exist versus just knowing about the practices. This, in turn, raises questions about whether or not, without this understanding, they will consistently make appropriate password choices across technologies and technological applications.

Bridging gap between knowledge and behavior

Further, this study reveals that children have appropriate perceptions and knowledge of passwords, but also demonstrate bad password habits that are contradictory to this knowledge. Students as young as third grade understand that passwords provide access controls, protect their privacy, and ensure their *stuff'*s safety. They also practice some good password practices such as memorizing passwords, limiting writing passwords down, keeping their passwords private, and logging out after sessions. However, many students exhibit password behaviors that do not align with their stated understanding of passwords, such as sharing passwords with friends, reusing passwords and using personal information when creating passwords.

This gap between students' stated password knowledge and their password behavior is an important next step for research surrounding children's password use and education. More mixed methods studies with more extensive questioning methods like interviews are needed to help better understand the nuances of children's perceptions of passwords, as well as the gap between knowledge and use. Understanding these nuances is important for thinking about how to better educate students about password behavior and online privacy and security, and how to move their knowledge into appropriate practice.

References

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Communications of the ACM*, 42(12), 41-46.

[2] Monica Anderson, and Jingjing Jiang. Teens, social media & technology 2018. *Pew Research Center* 31 (2018): 2018. Retrieved September 17, 2019 from https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/

[3] Sezin Baysal Berkup. 2014. Working with generations X and Y in generation Z period: Management of different generations in business life. *Mediterranean Journal of Social Sciences* 5.19 (2014): 218.

[4] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *2012 IEEE Symposium on Security and Privacy.* 538–552. DOI:http://dx.doi.org/10.1109/SP.2012.49

[5] Charles P. Bourne and Donald F. Ford. 1961. A Study of the Statistics of Letters in English Words. *Information and Control*, 4(1): 48-67, 1961.

[6] Yee-Yin Choong. 2014. 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.

[7] Yee-Yin Choong, Mary F. Theofanos, and Hung-Kung Liu. 2014. *United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study*. NISTIR 7991, 2014.

[8] Yee-Yin Choong and Mary F. Theofanos. 2015. 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. Springer, Cham. 2015.

[9] Yee-Yin Choong, Mary F. Theofanos, Karen Renaud, and Suzanne Prior. 2019. Case Study–Exploring Children's Password Knowledge and Practices. In *Workshop on Usable Security and Privacy (USEC) 2019.*

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

[11] Common Sense Media. 2019. The Common Sense Census: Media Use by Tweens and Teens, 2019. Retrieved from

https://www.commonsensemedia.org/Media-use-by-tweens-and-teens-2019-infographic

[12] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. 2010. Password Strength: An Empirical Analysis. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM).*

[13] EU Kids Online. 2014. *EU Kids Online–Findings, methods, recommendations*. LSE, London: EU Kids Online. Available on http://lsedesignunit.com/EUKidsOnline.

[14] Dinei Florêncio and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. In: *Proceedings of the 16th International Conference on World Wide Web*, pp. 657-666. ACM, 2007.

[15] Paul Grassi, James L. Fenton, Elaine M. Newton, Ray A. Periner, Andrew R. Regensheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, and Mary F. Theofanos. 2017. *Digital identity guidelines: Authentication and lifecycle management.* Technical Report 800-63B, NIST Special Publication, 2017.

[16] Libby Hanna, Kirsten Risden, and Kristin J. Alexander. 1997. Guidelines for usability testing with children. *interactions*, 4(5):9–14, 1997.

[17] Eiji Hayashi and Jason Hong. 2011. A Diary Study of Password Usage in Daily Life. In *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11*). ACM, New York, NY, USA, 2627–2630. DOI:http://dx.doi.org/10.1145/1978942.1979326.

[18] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lo´pez. 2012. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. 523–537.

[19] Sture Holm. 1979. A simple sequentially rejective multiple test procedure. *Scandinavian journal of statistics*, pp.65-70. 1979.

[20] Gunther Kress. 1997. *Before writing: Rethinking the pathway into writing*. Routledge.

[21] Dev Raj Lamichhane and J C. Read. 2017. 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.

[22] Paul Y. Lee and Yee-Yin Choong. 2015. 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.

[23] Michael P. Irwin. 2012. *An Investigation of Online Threat Awareness and Behaviour Patterns Amongst Secondary School Learners.* Doctoral dissertation, Rhodes University, Grahamstown, South Africa.

[24] Priya Kumar, Shalmali M. Naik, Utkarsha R. Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, *1,* CSCW, 64.

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

[26] Stuart MacFarlane, Janet Read, Johanna Höysniemi, and Panos Markopoulos. 2003. Half-day tutorial: Evaluating interactive products for and with children. In *Interact*, pages 1027–1028, 2003.

[27] Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. 2018. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children* (pp. 539-544). ACM.

[28] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie F. Cranor, Patrick G. Kelley, Richard Shay, and Blase Ur. 2013. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security,* pp. 173-186. ACM, 2013.

[29] Oxford Royale Academy. 7 Unique Characteristics of Generation Z. (January 25, 2018). Retrieved September 06, 2019 from https://www.oxford-royale.co.uk/articles/7-unique-characteristics-generation-z.html

[30] Ugnė Paluckaitė, and Kristina Žardeckaitė-Matulaitienė. 2017. Adolescents' Perception of Risky Behaviour on the Internet. In *ICH&HPSY 2017: The European proceedings of social & behavioural sciences EpSBS: 3rd icH&Hpsy international conference on health and health psychology, July 5-7, 2017, Porto. London: Future Academy, 2017, vol. 30.*

[31] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let's

go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17*), 2017.

[32] Marc Prensky. 2001. Digital natives, digital immigrants. *On the Horizon,* 9(5), 2001. Retrieved from https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

[33] Janet C. Read, and Brendan Cassidy. 2012. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children* (pp. 200-203). ACM.

[34] Karen Renaud and Joseph Maguire. 2015. 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.

[35] KwangCheol Rim, and SoYoung Choi. 2015. 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.

[36] Johnny Saldaña. (2015) *The coding manual for qualitative researchers* (3rd Ed.). SAGE Publications.

[37] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS'14*), July 2014.

[38] The Digital Future Report. 2018. *The 16th annual study on the impact of digital technology on Americans***.** Center for the Digital Future at USC Annenberg , Retrieved September 17, 2019 from https://www.digitalcenter.org/wp-content/uploads/2018/12/2018-Digital-Future-Report.pdf

[39] United States Department of Education. 2019. *The condition of education, 2019.* National Center for Education Statistics. Retrieved September 21, 2020 from https://nces.ed.gov/pubs2019/2019144.pdf

[40] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!' at the End to Make It Secure": Observing password creation in the lab. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15*), 2015.

[41] Blase Ur, Patrick G. Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. 2012. How does your password measure up? the effect of strength meters on password creation. In *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12),* pp. 65-80, 2012.

[42] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Proceedings of the 12th USENIX Conference on Us- able Privacy and Security (SOUPS '16*), 2016.

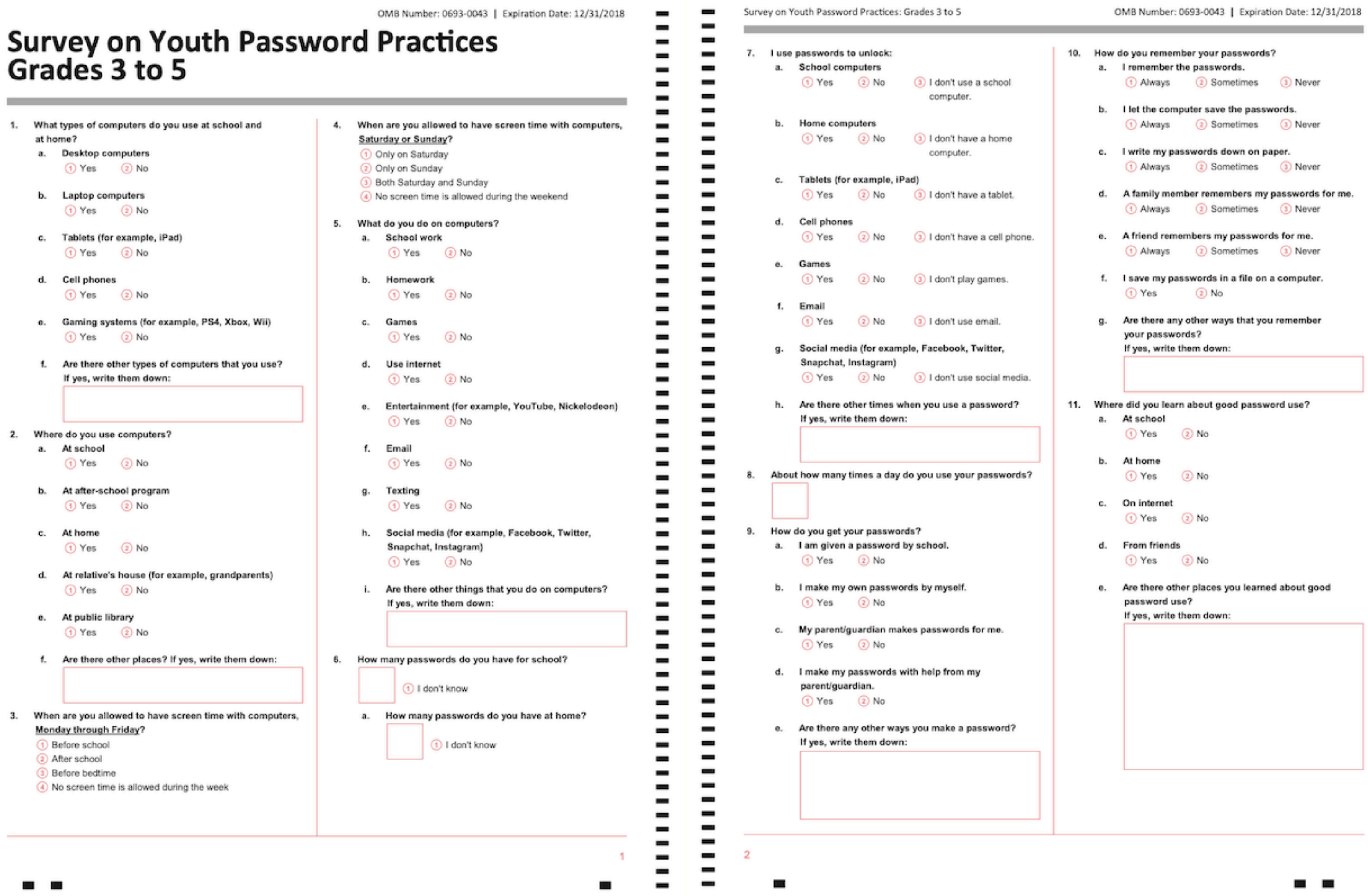
[43] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. 2004. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2(5):25–31, September 2004.

[44] Ramazan Yilmaz, Fatma Gizem Karaoğlan Yilmaz, H. Tuğba Öztürk, and Tuğra Karademir. 2017. Examining Secondary School Students' Safe Computer and Internet Usage Awareness: an Example from Bartin Province. *Pegem Eğitim ve Öğretim Dergisi, 7*(1), 83-114.

[45] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (pp. 388-399). ACM.

[46] Janko Žufić, Tomislava Žajgar, and S. Prkić. 2017. Children online safety. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 961-966). IEEE.

Appendix: Survey Instrument



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:

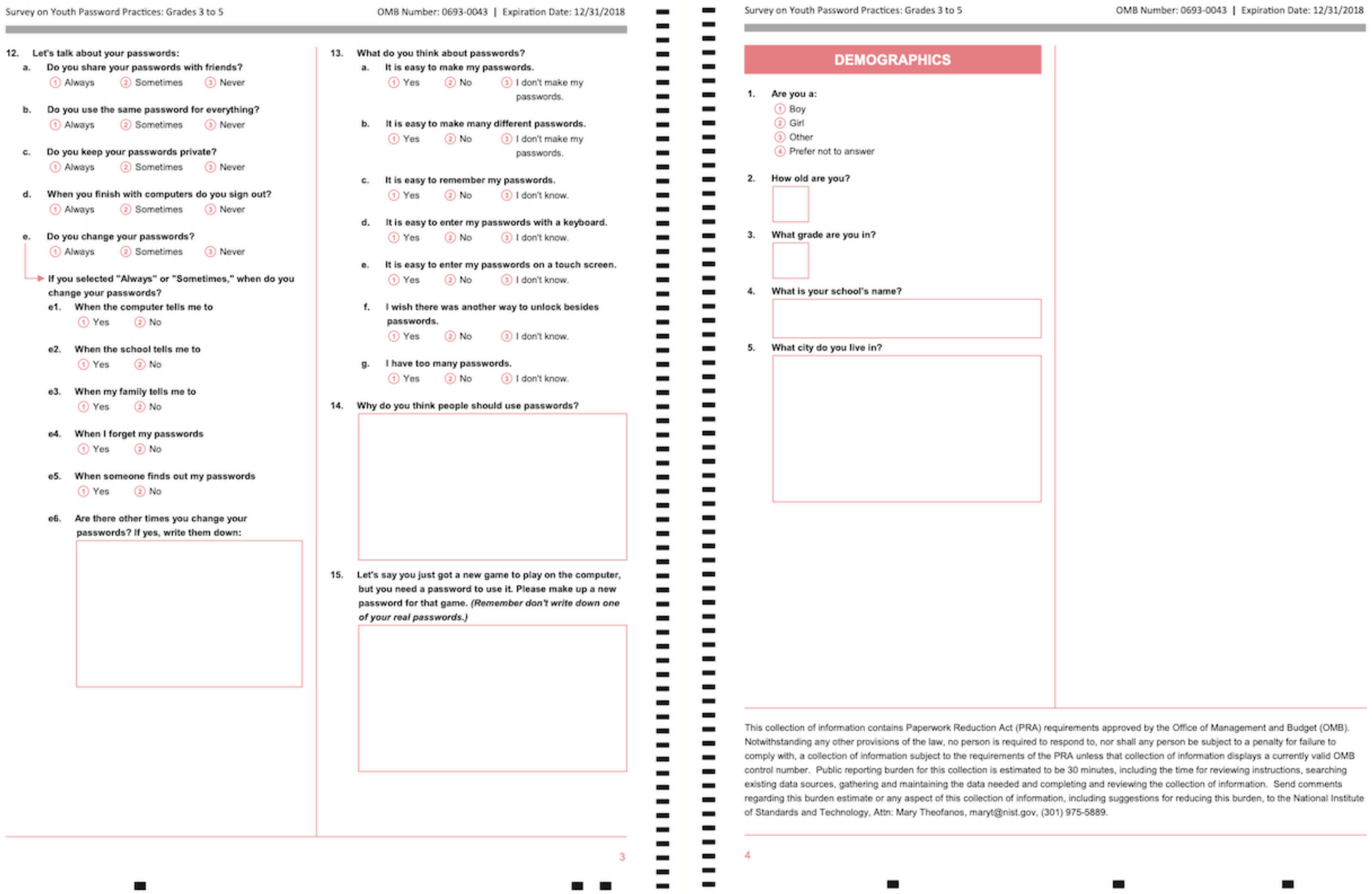
8. About how many times a day do you use your passwords?

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?

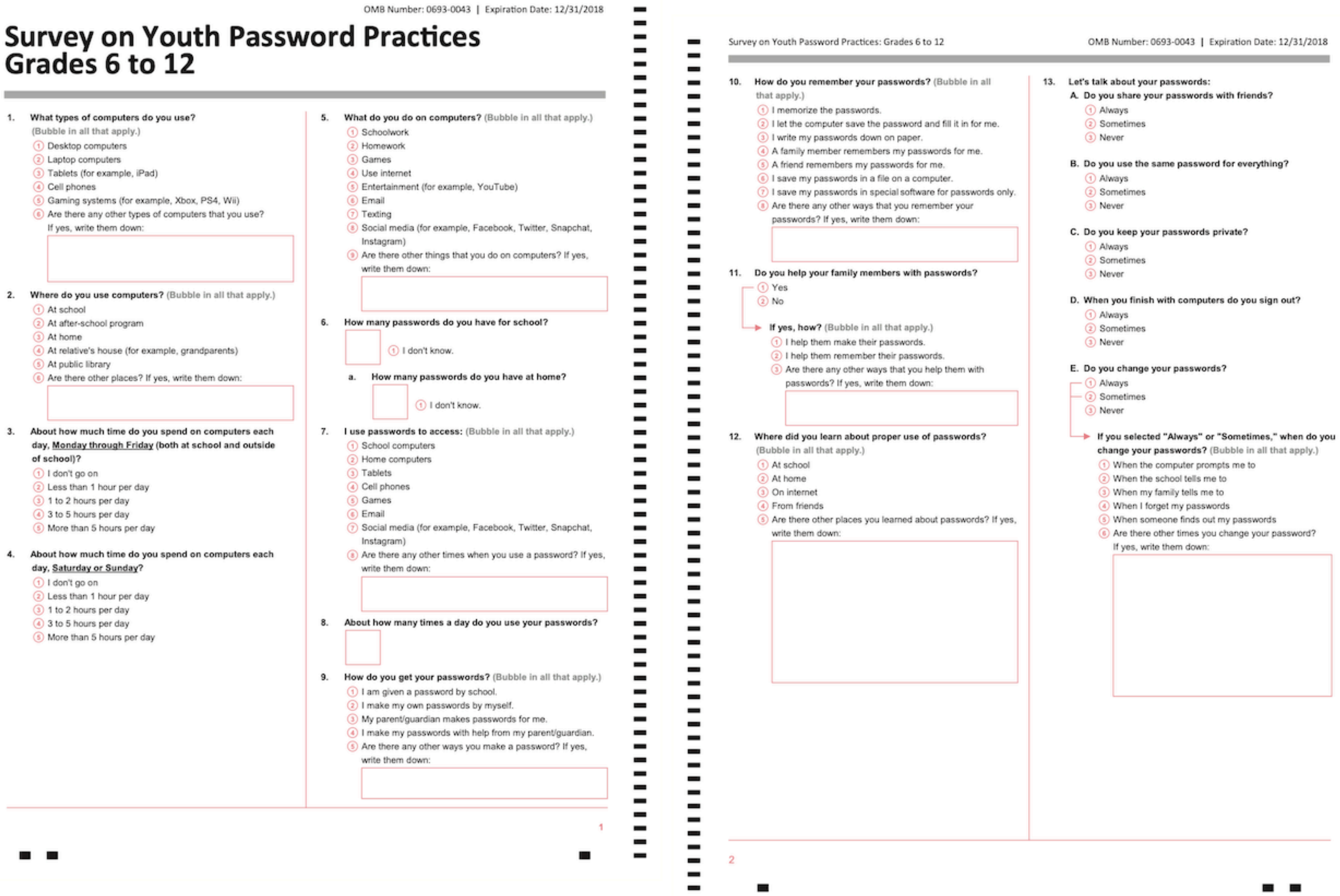
3. What grade are you in?

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



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

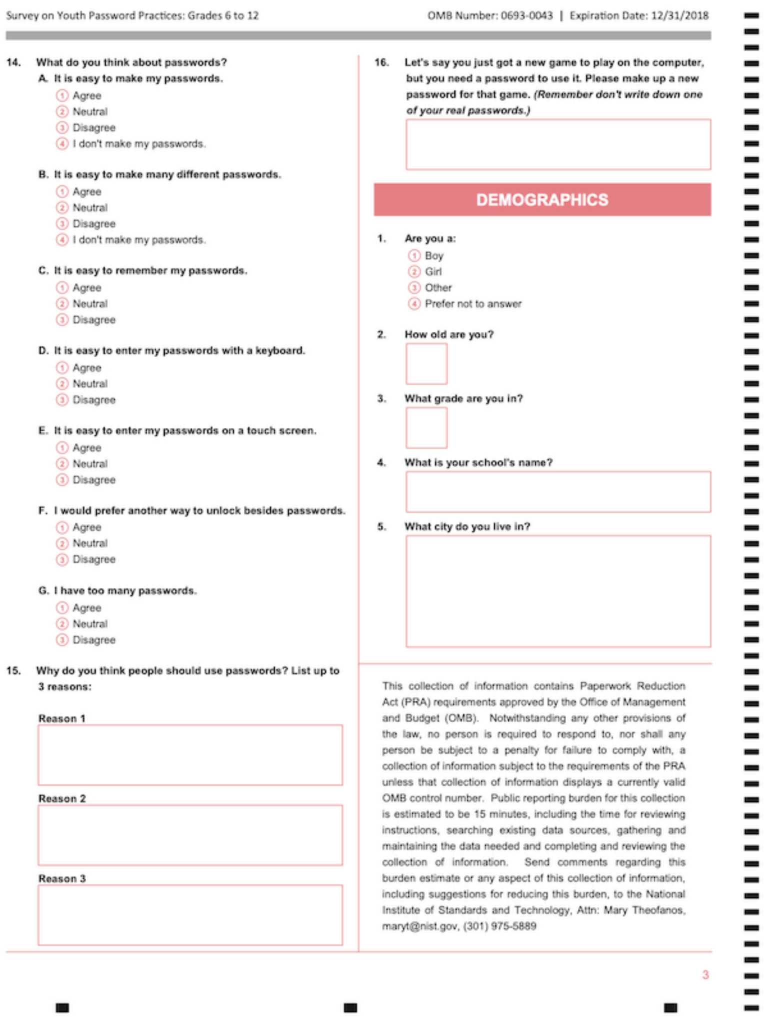
    C. **Do you keep your passwords private?**
    ① Always
    ② Sometimes
    ③ Never

    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