Parents, Passwords, and Parenting: How Parents Think about Passwords and are Involved in Their Children's Password Practices

Yee-Yin Choong[1]([✉]) [ID], Kerrianne Buchanan[1] [ID], and Olivia Williams[2] [ID]

[1] National Institute of Standards and Technology, Gaithersburg, MD, USA
{yee-yin.choong,kerrianne.buchanan}@nist.gov
[2] University of Maryland, College Park, MD, USA

Abstract. Though much is known about how adults understand and use passwords, little research attention has been paid specifically to parents or, more importantly, to how parents are involved in their children's password practices. To better understand both the password practices of parents, as well as how parents are involved in their children's password practices, we conducted a survey study of 265 parents in the United States (US) with school-aged children (kindergarten through 12th grade, 5 to 18 years old). We asked parents about their general technology use, the kinds of technologies and password-protected accounts they have; how they make and maintain their passwords; and about how, if at all, they help their children create and maintain passwords. We found that parent password practices align with research surrounding adult password practices, and that parents, especially those of younger children, are very involved in the creation and maintenance of their children's passwords. With these findings, we conclude with both recommendations for future research, as well as a call for the cybersecurity community to better support parents' password understandings and practices so that parents can better support their children.

Keywords: Privacy and Online Security · User Survey · Usable security · Passwords · Parenting

1 Introduction

Passwords continue to be the de facto authentication method for most devices and accounts that a typical digital user accesses online. Over time, these "typical digital users" have increasingly come to include youth at younger ages. These youth use a variety of technologies every day, sometimes for more than eight hours a day [20]. In doing so, they access dozens of security measures, applications, and accounts that all require the creation, use, and maintenance of passwords [20]. As youth age, the number of passwords they require—and the sensitivity of the data that those passwords

protect—increases, and the password practices they learn at a young age can turn into habits over time. The ubiquity and importance of passwords in youth's online lives demands an understanding of how children are using passwords. An important facet of this understanding is knowing more about from where youth password knowledge comes.

Parents and guardians[1] are often the first external point of contact in a child's password learning journey. Most youth's earliest exposure to technology and passwords happens under the supervision of their parents or guardians. Examining what parents know and how they are involved in their children's passwords is an important starting point for understanding how and from where children develop password understandings and behaviors. While we have an idea of what children do online [20, 23], and we know that parents are actively involved in children's online lives [13], there is still much to learn about the development of children's knowledge and behavior regarding the use of passwords, and the role parents play in this learning process. We designed this study to provide insights on how parents can best support their children's password practices by answering two research questions: RQ1–What are parents' password practices? and, RQ2–How, if at all, are parents involved in their children's password creation and maintenance? If so, does parental involvement differ across children's grade bands?

When conceptualizing this study, we found it important to ask parents not only about their involvement with their children's passwords, but also about their own password practices. This choice was made for two reasons: one, we wanted to know if there was something about the experience of being a parent that influenced their own password behavior, for example, being responsible for a young person's information online in addition to their own. Two, we wanted to see if and how parents were involved with their children's password creation and maintenance in order to understand more about parents' conceptualizations of youth's password needs. We also explored whether parent's involvement depended on the age of their child.

2   Related Research

The existing body of literature concerning password behaviors, password understandings, and password policies is enormous. To situate our current study of parents and their involvement in their children's password behavior in this vast landscape, we first synthesize recent literature regarding adult password knowledge and behavior, as most parents are also adults. Then we explore studies that address the same understandings in youth. Finally, we examine the few studies that investigate the role that parents play in youth password knowledge to lay the groundwork for our exploration of parents' password behavior and their involvement in their children's password practices.

2.1   Adults' Password Habits

Although most adults are generally aware of basic password hygiene [1], studies find that many adults still enact undesirable password behaviors [10, 16, 26]. Some research

---

[1] Both parents and legal guardians are referred to as "parents" hereafter throughout the paper.

suggests these undesirable behaviors stem from flawed password creation beliefs [28], such as believing that the inclusion of a symbol like an "!" automatically increases security [28], or that reusing passwords is acceptable if those passwords are strong [15]. Multiple studies have found that re-use of passwords is especially common [5, 17, 31], indicating that adults struggle to balance security, usability, and convenience in having many passwords for a variety of devices and accounts [6, 24, 25].

Indeed, many studies have shown that this cognitive dissonance between usability and security in password priorities results in users who know good password and security behavior but do not enact them [30]. For example, Ur et al. found that participants perceived a tradeoff between security and memorability, rating more secure practices as more difficult to remember [29]. In such cases, if users valued the usability of a password—i.e., the ease of remembering and entering it into a website or device—more than security, they were likely to sacrifice some level of security even if they knew what secure behaviors were [18, 32]. A study of 902 participants' adoption and/or abandonment of 30 common security practices found similar results, such that participants ignored or deserted good practices due to inconvenience, low perceived value, or because they just thought they knew better [34]. These findings collectively suggest that understanding good password behavior, alone, is a far cry from ensuring good password practice.

Because most parents are also adults, these findings about adult password behavior both inform an understanding of parent password behavior, while also raising further questions. It is unclear whether parental responsibilities—such as having to help teach children about passwords or being generally responsible for the online privacy and security of others—are related to one's own password knowledge and practice development. It is also unclear whether and how parents' complex and sometimes disjointed password understandings and practices are related to their conceptualization of appropriate password practices for themselves and for their children. Our study aims to contribute to these understandings.

2.2   Youth Password Knowledge and Behavior

Like their adult counterparts, there seems to be a gap between what children understand in theory and what they practice in real life [4, 11, 19]. For example, Zhang-Kennedy et al. found that study participants (7 to 11-year-olds) had good foundational password knowledge, such as knowing that they should not share their passwords with strangers and that passwords are secrets [33]. However, these participants had conflicting behavior, like one participant who stated the importance of not sharing passwords with anyone including family members, but who also reported that their mother had made their password for them, and later shared one of their passwords with the researchers [33].

Other studies have noted developmental trends in youth password habits; while youth may know that complex passwords are important, from a developmental standpoint, they may not be ready to create and reliably use them [12]. Moreover, some studies have found that password understandings and behavior change over time. For example, a study of 1,505 3rd to 12th grade students revealed that while middle and high school students were more likely to report that they keep their passwords private, they were also significantly more likely to report sharing their passwords with friends and using the same password across multiple accounts than their elementary school counterparts

[27]. Other studies suggest that the older children get and the more passwords they have to make and maintain, the more some of their habits tend to reflect those of adults [21].

Fortunately, children's password knowledge and behavior are in constant development, and thus can be changed with support, good information, and encouragement. For instance, in a password simulation activity, Maqsood et al. found that their 20 pre-teen participants believed that their simple passwords containing personal information were secure. But when participants were introduced to the rule and value of including special characters in password creation, the participants quickly understood [14]. As a result of their study, Maqsood et al. leveraged a call for "further studies with parents [to] explore their knowledge of secure passwords and what they teach their children about the topic" (p.543) [14]. As social learning theory supports that children's learning is a direct result of their environment and the people in it [3], and parents are the first and often most prominent figures in children's environments, we agree with Maqsood et al. that exploring what parents teach children about passwords is important. Our current study of parents' password knowledge and their involvement in their children's password behavior is a direct answer to this call.

2.3   The Involvement of Parents in Youth Password Behavior

There is little research dedicated to understanding the involvement of parents in their children's password behavior, but those studies that do exist lay important groundwork for this study. They find, first and foremost, that parents actively choose to involve themselves in their children's password creation [19]. From the children's perspective, Choong et al. found that many elementary school children reported having parental help with password creation and tracking [4]. From the parent perspective, in Zhang-Kennedy and colleagues' 2016 dyadic study of parent/child perception of cyber threats, all 14 of the study's parent participants reported controlling their young (7–11 years old) children's passwords and accounts and talking with their children about how to create passwords [33]. Unfortunately, parents reportedly felt torn between wanting to teach their kids good behavior with the reasoning behind that behavior and wanting to shield their children from the harsh realities of the world. For example, some of the advice these parents provided to their children included choosing a weaker but easier to remember passwords [33].

Our study builds onto this limited body of work by focusing on a larger sample of parents and extending the grade range of children to include kindergarten through 12th graders. As described earlier, children's learning can be influenced directly from their parents [3]. If parents are involved in passing down their password knowledge to their children, understanding more about how this involvement happens is an important precursor of understanding children's password knowledge and behavior. Our study examines the password understandings and practices of a larger group of parents, looks for trends in parent involvement in children's password creation and maintenance across several developmental stages, and explores how, if at all, parents' own practices are impacted by working with their children.

3   Methods

To answer our two research questions, we conducted an online survey study with US parents of children from kindergarten to 12th (K-12) grades (typically 5 to 18 years old).

3.1   Survey Development

Guided by our two research questions, the objective of the survey was to gather information on household technology use, parents' password practices, and parents' involvement in their children's password practices.

We developed a list of survey items based on findings from literature and past studies. Three types of reviews were conducted iteratively. Content experts in usable security evaluated and provided feedback on the alignment of survey items with the scope of the survey goals. Survey experts reviewed each item for clarity for the intended audience, appropriate format, and alignment of response options. Then, cognitive interviews with parents were conducted using a talk-aloud protocol to determine if questions were being appropriately interpreted. The survey instrument was refined iteratively based on the feedback from each type of review. The final survey was implemented by a contracting research firm to collect responses online. The survey was divided into two major sections, corresponding to the two research questions.

Parents' Password Practices.   There were seven sets of questions to address RQ1.

1. Family devices (*desktop computers, laptops, tablets, cell phones, game consoles, smart TVs*), number of devices owned and number of password-protected devices
2. Number of personal accounts across eight account types (*email, social media, banking, shopping, bill payment, entertainment, games, accounts related to children*) and number of accounts requiring passwords
3. Number of personal passwords
4. Password creation:
   a. Importance of considerations (*easy to remember, easy to type, strong–hard to crack, same as other passwords*)
   b. Whether password generators are used (*Always, Sometimes, Never but know about it, Never and don't know about it*)
   c. Create a password for a hypothetical account on family doctor's website
5. Password tracking and maintenance:
   a. Methods used to keep track of personal passwords (*memorize, browser/device saved and auto-filled, use mnemonics, someone else remembers, write on paper, save in files, save in emails, password manager, do not track*)
   b. Frequency of changing personal passwords (*30, 31–60, 61–90, 91–120, 121–180 days, change only when necessary, change depending on accounts*)
6. Sources for password help and perceived effectiveness of those sources (*family members, friends, internet provider, account websites, internet search, media, paid technical support, public library, children's school, government agencies*)
7. Technology landscape: usage, technology savviness, technology adoption
   a. Daily hours spent on computers/devices (*< 1, 1–3, 3–5, 5–7, 5–9, > 9*)
   b. Technology savviness (response options in Table 1)

c. Technology adoption (response options in Table 1)

Technology savviness and adoption responses were labeled to aid in statistical data analysis and discussion. The response options and their labels are shown in Table 1.

Table 1. Labels for Technology Savviness and Adoption.

Technology Savviness	
Labels	Response Options
Novice	*I have limited experience using technology and I don't know much about how technology works*
Average	*I have some knowledge about how technology works, but often need to ask for help to perform more advanced activities – such as to configure the privacy settings on my cell phone*
Advanced	*I can do most things that I want to do with technology and only need help occasionally*
Expert	*I can do all things that I want to do with technology without help from others*
Technology Adoption	
Labels	Response Options
Laggard	*I only adopt new technologies when it's required*
Late majority	*I wait until my old technology dies*
Early majority	*I let others work out the kinks first*
Early adopter	*I follow technology trends*
Innovator	*I try the latest technologies as soon as they come out*

Parents' Involvement with Children's Passwords. There were three sets of questions. to address RQ2. This section was repeated for each child within the grade range of K-12 as reported by a parent participant. For parents with more than one child, they had the option to select if their answers were the same (if "*same*", then the question block was skipped for that child) or different from a previously entered child.

1. Do you help this child create passwords? (*Always, Sometimes, Never*)
   a. If *Always* or *Sometimes*, how (check all apply)?

   - *I create passwords for this child.*
   - *This child and I work together to create his/her passwords.*
   - *I only give this child guidance, but he/she creates the passwords.*

b. If *Always* or *Sometimes*, rate the importance of considerations when helping this child with password creation (*easy to remember, easy to type, strong–hard to crack, same as other passwords*)

2. Do you help this child keep track of passwords? (*Always, Sometimes, Never*)
   a. If *Always* or *Sometimes*, how (check all apply)?

   - *I have a list (paper or electronic) of this child's passwords.*
   - *I memorize this child's passwords.*
   - *I have this child create a list of passwords and he/she is responsible for keeping the list.*
   - *I give this child guidelines on how he/she should keep track of the passwords.*

3. Has helping your children with their passwords changed your own password practices? (*Yes–why, No–why not?*)

3.2 Participant Sampling and Demographics

The study was approved by our institution's Research Protections Office and the Institutional Review Board (IRB). All responses were collected anonymously.

We used a research firm for participant sampling utilizing double opt-in research panels. Panelists were notified about the survey through online advertisements. Interested panelists were qualified if they met these criteria at the time of taking the survey: (1) be at least 18 years old; (2) reside in the US; (3) be parents or legal guardians; (4) have at least one child within the K-12 grade range. Participants received proprietary internal currency that, while not equating to an exact dollar-for-dollar value, holds monetary value of approximately $1 US dollar.

A total of 265 panelists self-selected to complete the survey; 82.64% were female and 17.36% male. A majority of the parents were under 45 years old (18–34: 30.42%; 35–39: 20.91%; 40–44: 16.73%; 45–49: 15.97%; 50 or older: 15.97%). Nearly a third (32.95%) of parents had a Bachelor's degree, 29.50% had less than high school or a high school degree, 19.92% had an Associate's degree or some other degree, and 15.71% had an advanced or professional degree.

A majority of the parents had one (n = 136, 51.32%), two (n = 87, 32.83%), or three (n = 32, 12.08%) children within the target grade range of K-12. Only 10 parents (3.77%) had four or more children. Parents were asked to indicate each of their children's grade and sex. Grades were categorized into three grade bands: Elementary school (ES)–kindergarten through 5th grade; Middle school (MS)–6th through 8th grade; High school (HS)–9th through 12th grade.

This paper focused on data and results of the first child parents entered the survey, as the majority of parents only had one child, and parents with more than one child tended to report that their answers for subsequent children in their family were the same as their answers for the first child. For parents with two children, answers only differed from the first child for 23 parents (26.44%). For parents with 3 or more children, only 15 (34.88%) differed from a previously entered child. Future efforts will examine patterns between and across parents with multiple children. Table 2 shows percentages of the grade bands and sex of the parent participants' first child reported.

Table 2. Demographics of First Child Reported (n = 265)

Grade Band (%)			Sex (%)	
ES	MS	HS	Boy	Girl
47.55	21.89	30.56	52.34	47.66

Each participant was assigned a unique alphanumerical identifier, for example, p123456789. In this paper, any quotes provided as exemplars are verbatim from survey responses and presented in italics with its unique participant identifier.

3.3 Data Analysis

Primary Analysis. We used descriptive statistics to examine participants' responses to survey questions. For categorical questions, we computed frequencies and percentages for parents' responses to each question. For variables with continuous data, we computed averages (i.e., accounts requiring passwords, personal passwords, password tracking strategies). We also examined the relationship between continuous variables with a correlation. The strengths of hypothetical passwords created were scored using the zxcvbn.js[2] script, an open-source tool which uses pattern matching and searches for the minimum entropy of a given password. Password strength was measured by assigning passwords with scores ranging from 1 to 5, with 1 as the lowest strength.

We used inferential statistics to find significant differences between demographic subgroups in the data. We examined if parent password behaviors depended on parents' demographic characteristics (i.e., sex, age range, education, technology savviness, and technology adoption). We also examined if parents' involvement with their child depended on the child's grade band. We report Chi-square tests (the statistic, degrees of freedom, and p-value), which evaluated significant differences between groups on categorical outcome variables.[3] Significant Chi-Square tests were followed up by examining adjusted standardized residuals [2, 22]. Wilcox and Kruskal-Wallis non-parametric tests were conducted for responses measured on an interval scale (e.g., password strength) and/or were not normally distributed (e.g., number of password tracking strategies). Significance for all inferential tests was determined using an adjusted alpha level of $\alpha = 0.01$ and all effect size estimates were calculated using Cramer's V. All significant effects had effect sizes ranging from small to moderate. In this paper, only statistically significant test results are presented.

Because all survey questions were optional, only valid responses were used in analyses. Thus, the total number of responses differed for each question. Additionally, as stated previously, analysis was conducted on the first child parents entered the survey.

Post Hoc Tests. We also examined the association between parents' password priorities and parents' priorities for their child's passwords. We conducted a Chi-Square test to

---

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

[3] In cases in which the Chi Square test could not be run due to small cell sizes, Fisher's exact tests were conducted. In some cases, p-values were simulated to ascertain statistical significance.

examine this association for the four password priority items. Significant tests were followed up by examining the adjusted standardized residuals.

4   Results

4.1   Technology Savviness and Adoption

Parents in the study tended to report as savvy with technology (Fig. 1), with over 86% reporting having advanced or expert experience. Figure 1 also shows that most parents reported as "*early majority adopters*" or "*early adopters*" of technology.
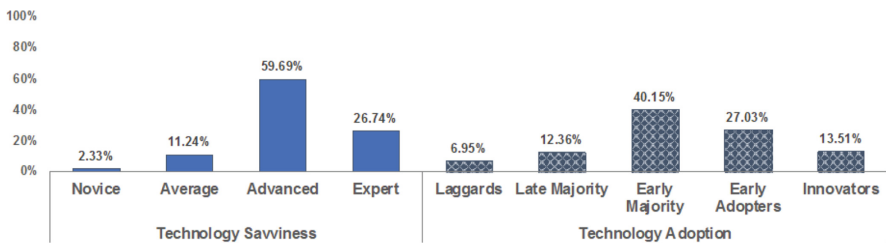
Fig. 1. Parents' self-reported technology savviness and adoption

4.2   Parents' Personal Devices, Accounts, and Passwords

We examined parents' ownership and password protection of six different device types: cell phones, tablets, laptops, game consoles, smart TVs, and desktop computers. For each, we calculated the percentage of parents who owned at least one of the device types and the percentage of parents who password protected at least one of the device types. A majority of parents owned each of the six devices asked in the survey with high ownership (over 85%) of having cell phones, tablets, and laptops (Fig. 2).
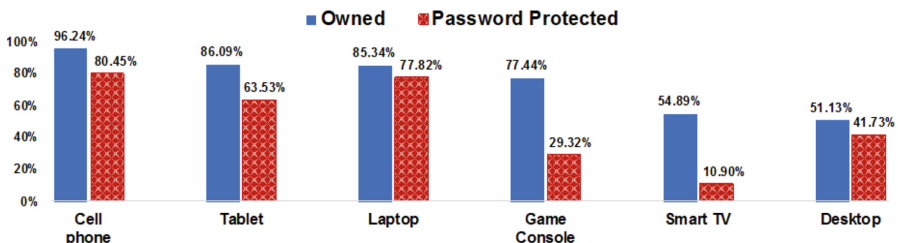
Fig. 2. Parents' ownership and password protection of devices

However, fewer parents reported password protecting their devices than owning devices (Fig. 2). For example, while 96.2% of parents owned a cell phone, only 80.5%

reported password protecting a cell phone. This suggests some parents do not always password protect their devices.

The survey asked parents for their total number of personal passwords and the number of online accounts they had that require passwords. Parents reported an average of 10.5 personal passwords (SD = 13.5, range: 0–99), and 15.9 accounts (SD = 14.7, range 0–128) requiring passwords. Parents' personal passwords were significantly correlated with the number of accounts requiring passwords ($r = 0.63, p < .01$). Further, the number of personal passwords is smaller than the number of accounts requiring passwords. This indicates personal passwords may be reused for some accounts.

4.3 Parents' Password Behaviors

Password Priorities. A majority of the parents believed it was important for passwords to be both easy to remember (80.4%) and strong (75.5%), as shown in Fig. 3. To a lesser extent, parents also believed it was important for passwords to be easy to type (49.1%) and be the same as others (33.2%).
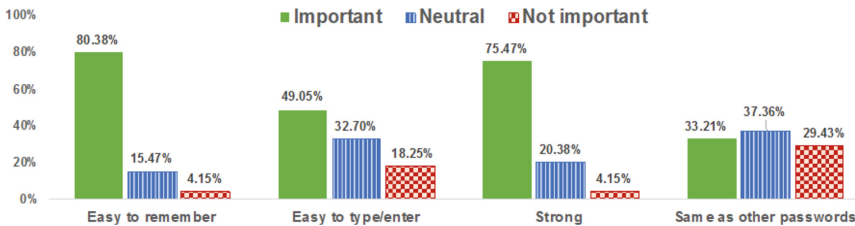

Fig. 3. Parents' priorities for own passwords

Password Generators. Fewer than 20% of parents used password generators when creating their personal passwords. While some (41.7%) had heard of password generators, nearly as many (39.1%) were not aware password generators existed.

We found a significant effect of parents' reported technology adoption on use of password generators ($\chi^2(6) = 21.5, p < .01$). Parents reported different levels of technology-adoption: from being very interested in new technology (e.g., "*innovator*" and/or "early adopter") to not interested at all (e.g., "late majority" and/or "laggard"). The examination of the adjusted standardized residuals revealed that more "*innovator*" parents used password generators (choosing options "*Always*" or "*Sometimes*"), and fewer reported "*Never, although I know about the existence of those password generators*"; fewer "*late/laggard*" parents used password generators (choosing options "*Always*" or "*Sometimes*"). More "*early adopter*" parents reported "*Never, although I know about the existence of those password generators*". This suggest parents who reported following and trying the latest technology were, if not using, at least more aware of password generators.

Password Tracking Strategies. Parents on average chose two of the 13 listed methods as how they track their passwords (SD = 1.1, range = 0–6). A majority of parents used

memorization techniques (mnemonics or memorized passwords; 78.5%). To a lesser extent, parents used technology (browser/device autofill or password management software; 43.0%), physically wrote down passwords (37.7%), or saved their passwords electronically (e.g., email, file; 17.4%). Nearly 1 in 10 parents (9.1%) also reported using the "forgot password" feature instead of tracking passwords.

We found significant effects of parents' reported technology adoption ($\chi^2(3) = 11.5$, $p < .01$) and age ($\chi^2(4) = 20.8$, $p < .01$) on use of memorization techniques to track passwords. Analysis shows fewer "*late/laggard*" parents used memorization techniques to track their passwords. Additionally, across age ranges, more parents between 18 and 34 years old and fewer parents over 50 years old used memorization techniques to track their passwords. This suggests older parents and those who reported being less interested in adopting new technology do not tend to use memorization techniques.

Frequency of Password Change. A majority of parents (53.4%) changed their passwords only when necessary. Over a third of parents (34.2%) changed their passwords between 30 and 180 days and 12.4% changed their passwords depending on the account type.

Passwords Generated for Hypothetical Accounts. Passwords generated for a hypothetical account were on average 10.71 characters in length. Most parents used lowercase letters (59.5%) and numbers (23.0%), and fewer used uppercase letters (10.8%), symbols (6.1%), and white space (0.5%). Very few parents (4.7%) had lowest strength passwords (score = 1), and only 22.8% had a password scored at the highest level (score = 5). Thus, most parents (72.5%) created password with strength scores ranging from 2 to 4 (out of 5).

How/Where to Seek Password Guidance. Parents sought a variety of sources for information or guidance of passwords including family members (41.7%), internet searches (29.9%), and websites where accounts are created (23.9%). A majority of parents felt that each source was effective, with family members being rated as most effective (70.9%) followed by websites (60.3%) and internet searches (50.6%). However, for internet searchers, nearly as many parents were neutral (48.1%).

4.4 Parents' Involvement with Children's Password Creation

Helping Children Create Passwords. Parents tended to help their children with password creation. About 74% of parents ("*Always*": 33.0%; "*Sometimes*": 41.0%) helped their children with password creation, and 26.0% "*Never*" helped. However, parents' help significantly depended on their child's grade band ($\chi^2(4) = 35.2$, p < .01), with more parents helping younger children and fewer helping older children (Fig. 4).

More parents "*Always*" helped their ES child and fewer "*Sometimes*" helped. More parents helped with their MS child "*Sometimes*" and fewer "*Never*" helped. More parents "*Never*" helped their HS child and fewer "*Always*" helped.

Parent Strategies for Involvement with Child's Password Creation. Parents who "*Always*" or "*Sometimes*" (n = 189) helped their children with password creation did so in various forms. Most parents helped their child by creating passwords together (46.6%),
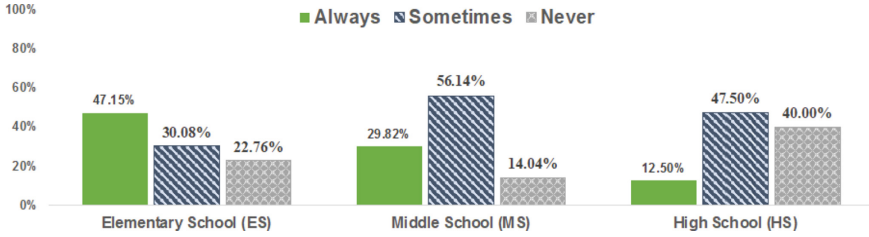
Fig. 4. Responses to "Do you help this child create his/her passwords" by child grade band.

but some created passwords for their child (29.6%) or gave their child guidance (25.4%). Few parents (1.1%) reported they helped their child in some "*other*" way.

The number of parents creating passwords for their child ($\chi^2(2) = 23.8$, $p < .01$) and giving guidance ($\chi^2(2) = 18.1$, $p < .01$) significantly differed depending on the child's grade band, but working together with the child did not. More parents created passwords for their ES child, and fewer parents did so for their MS or HS child. More parents gave their MS child guidance for password creation and fewer gave guidance to their ES child. Figure 5 displays parents' strategies for their involvement with their child's password creation by child grade band.
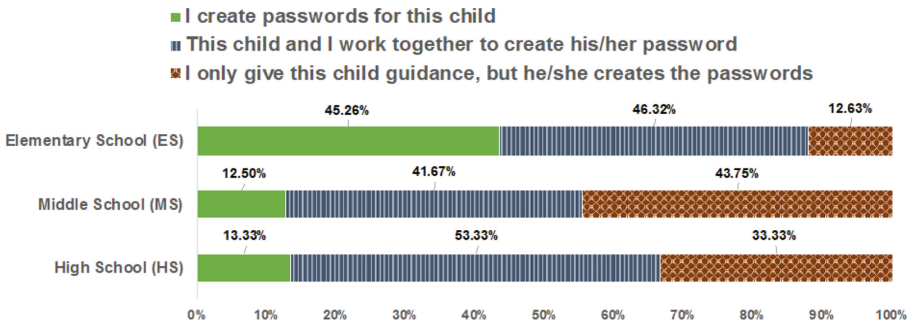

Fig. 5. Parent strategies for involvement with child's password creation by child grade band.

Password Priorities for Children. A majority of parents believed it was important for their children's passwords to be easy to remember (73.7%), strong (64.5%), and easy to type/enter (53.5%). About 30% of parents believed it was important for their children's passwords to be the same as other passwords (29.0%). When helping their children with password creation, parents' priorities significantly differed depending on the child's grade band for being easy to type ($\chi2(4) = 27.5$, $p < .01$), strong (Fisher's exact test $p < .01$), and the same as the child's other passwords ($\chi2(4) = 19.0$, $p < .01$). These differences are described below.

- **Easy to type.** More parents of ES children indicated it was important for their child's password to be easy to type and fewer were neutral. More parents of MS children were neutral for their child's password being easy to type and fewer indicated this

was important. More parents of HS children indicated this was not important for their child's password and fewer indicated it was important.

- **Strong.**[4] More parents of HS children indicated it was important for their child's password to be strong. More parents of ES children indicated this was not important or were neutral about this for their child's password.
- **Be the same.** More parents of ES children thought it was important for their child's passwords to be the same and fewer thought this was not important. More parents of MS children were neutral on this priority for their child. More parents of HS children thought this was not important and fewer thought it was important.

Post Hoc Test of Association of Password Priorities.   Parents' own password priorities and parents' priorities for their child's passwords were significantly related for being easy to remember ($\chi 2(1) = 57.1$, p $< .01$), easy to type ($\chi 2(1) = 49.8$, p $< .01$), strong ($\chi 2(1) = 71.2$, p $< .01$), and the same ($\chi 2(1) = 56.1$, p $< .01$). For all priorities, more parents thought that if the priority was important for their own passwords, it was also important for their child's passwords. Likewise, priorities not important to parents or if parents were neutral, they believed the priority was also not important or neutral for their child's passwords.

4.5   Parents' Involvement with Children's Password Tracking

Helping Children Track Passwords.   Almost 80% of parents (*"Always"*: 40.4%; *"Sometimes"*: 38.9) reported helping their children keep track of passwords and 20.8% reported that they *"Never"* helped with password tracking.

Parents' help significantly differed depending on their child's grade band ($\chi^2(4) = 38.2$, *p* $< .01$). More parents of ES children *"Always"* helped their child, and fewer *"Sometimes"* or *"Never"* helped. More parents of MS children *"Sometimes"* helped their child and fewer *"Always"* helped. Fewer parents of HS children *"Always"* helped their child and more *"Never"* helped. Figure 6 displays frequencies of help by child grade band.
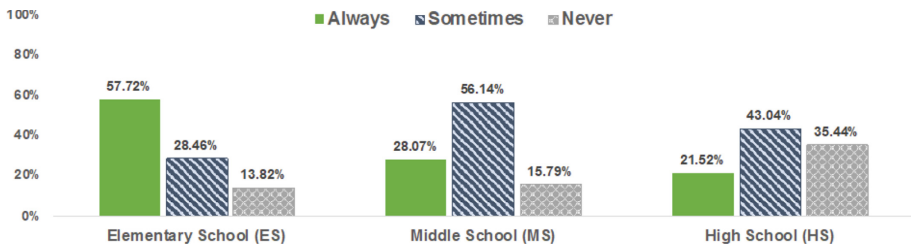
Fig. 6. Responses to "Do you help this child keep track of his/her passwords" by child grade band.

---

[4] Due to small cell sizes, "not important" and "neutral" items were combined for follow-up analysis. This yielded a significant Chi-Square $\chi^2(2)=12.9$, p$<.01$.

Parent Strategies for Involvement with Password Tracking. Parents who "*Always*" or "*Sometimes*" (n = 205) helped their children with password tracking did this in various ways. Most memorized their child's passwords (47.8%) or made a list of the child's passwords (43.4%). Few gave the child guidance for tracking (14.6%) or had their child create their own list they were responsible for (14.2%).

4.6 Has Helping Children with Passwords Changed Parents' Password Practices?

A majority of parents (80.38%) reported that they had not changed their password practices as a result of helping their children with passwords. However, changing password practices depended on parents' technology adoption ($\chi^2(3) = 17.736$, $p < .01$). More "*innovator*" technology adoption parents reported their password practices changed after helping their children with passwords, and fewer "*early majority*" technology adoption parents did.

Of those parents who reported that helping their children had not changed their own password behavior, 140 parents offered reasoning for why. For most, they believed they already had good password practices that they did not want to change, or they did not think it was important to change their current behaviors. For example, one parent commented that they were "*set in my ways with no need to really change*" (p558784107) while another explained that they "*already had enough ways to formulate various types of strong passwords*" (p55901423). Other common reasons were age-specific, as in the case of p100000982 who indicated that they were "*more capable of memorizing more complex passwords than my 5-year-old. Her passwords are much too simple for me to use and still feel like I am somewhat secure when I log in.*"

Only 19.62% of parents reported that helping their child has changed their own password habits, and 36 of them offered their reasoning. Some of these parents said working with their child served as a reminder of good habits, while the rest learned something new in the process. These new, learned behaviors included knowledge about how to make a strong password, information about how often passwords should be changed, insights into how to manage multiple passwords, and new memorization strategies.

5 Discussion

Research has well documented the password understandings and behaviors of adults (e.g., [32]) and more recently has started investigating the same behaviors in children (e.g., [27]). However, little attention has been given to how parents are involved in their children's password behaviors. The goal of this study was to examine the password behaviors of parents and their involvement with their children's passwords.

5.1 RQ1: Parents' Own Password Behaviors

Our first research question was to examine parents' password practices in order to gain insight into parents' password perceptions and practices. Although parents in this study

prioritized both high usability (easy to type, easy to remember) and high security (strong) for their passwords, our results indicate parents' practices may favor usability over security. For example, despite valuing strong passwords, a majority of parents created hypothetical passwords of moderate strength and containing mostly lowercase numbers and letters. Further, a large majority of parents in this study relied on memory and mnemonic strategies. Very few reported using password generators, which often produce passwords that are secure but may be difficult to type and remember. Additionally, parents in this study reported having more active accounts than personal passwords, suggesting a habit of reusing passwords. Wash and Rader suggests this behavior may be due to the challenge and cognitive difficulty of having many passwords [32]. Therefore, while parents desire passwords that are both strong and usable, practically they may be unsure how to achieve both goals simultaneously, especially given the large number of passwords they have and the current state of password requirements and guidance from technology providers [9]. This may result in parents placing more weight on practical usability than on high-level security when creating and maintaining passwords. Taken together, this suggests that parents (as well as users generally) can benefit from having more support and guidance for how to have both strong and usable passwords.

Indeed, our findings suggest parents may have few reliable sources of password guidance. Parents most often cited other family members as a key source of password guidance, which raises some practical questions. If parents struggle with balancing priorities and practices, but are themselves an important source of other family members' password guidance, how, when, and where are good resources for parent behaviors introduced and circulated? Additionally, our findings revealed few relationships between parent demographic characteristics (e.g., self-reported technology adoption) and password behaviors. Thus, it is unclear what qualities and experiences are related to alignment of priorities and practices.

Understanding parents' password perceptions and behaviors are important for examining if, how, and when these information are translated to their children. Given parents themselves have discrepancies between their priorities and practices, the study's next major goal was to examine parents' password approaches for their children.

5.2 RQ2: Parents' Involvement in Children's Password Behaviors

Parents in this study were involved in helping their children make and maintain passwords. Our study also shows that parents demonstrated developmental awareness when it came to helping their child with password creation strategies, tailoring help to their child depending on their age. For example, parents of ES children emphasized making passwords easy to type, while parents of HS children valued password strength. Further, differences in parents' reported involvement in password creation and maintenance with ES, MS, and HS children suggests that a gradual release of parental participation as children age. For example, parents reported often helping their ES child with passwords, but only helping MS and HS aged children sometimes or not at all. Involvement was also more direct (i.e., helping create and track the passwords) with ES children versus indirect (i.e., providing guidance or advice). Although this study was not longitudinal, the differences between parents' reported involvement depending on their child's age makes the gradual release theory worthy of further study. Developmental awareness and

the possible gradual release of password control to children over time are both encouraging parent practices. However, this raises the question of when, how, and why parents may replace the developmentally appropriate password behaviors targeted at younger children with strategies for strong, adult-appropriate password behaviors for older children? Future work examining parenting behaviors over time is encouraged to answer these questions.

Although the child's grade band was an important factor for parental involvement in password practices, our results also suggest that parent's own perceptions are related to how they approach their child's passwords. Parents' priorities for their own passwords aligned with their priorities for their child's passwords. For example, parents who believed it was important for their passwords to be easy to remember, easy to type, strong, and/or the same as other passwords found these same priorities important for their child's passwords. Similarly, when parents found these priorities to be neutral or unimportant for themselves, they also believed the priorities were neutral or not important for their child. This raises the question of how parents' perceptions are related to the child's own password practices and perceptions. If parents do not believe strong and/or usable passwords are important for neither themselves nor their child, are these beliefs transferred to their child? From this study alone, it is unclear if and to what extent, children learn and practice: a) their parent's own priorities, b) their parent's priorities for the child, or c) their parent's actual password behavior. Understanding how children's learning takes place may be important for understanding how parents can instill their children with effective password practices.

While the impact of parents on their child's practices needs further investigation, our study did find some evidence suggesting that helping children with passwords can change parents' own password practices. Although most parents did not change their password practices as a result of being involved with their child's passwords, nearly one in five did report changing their practices, with many reporting positive changes. This suggests it is worth exploring if there are important bidirectional effects between parents and their children on their password practices. Research examining both parents and their children together is needed to understand the impacts of parents' and children's' perceptions and behavior on one another.

5.3 Practical Implications

Our findings show that there is a strong need to help parents with their own password behaviors and with teaching password behaviors to their children. Because parents are a primary influence on children's perceptions, understandings, and behaviors [8], it is important that parents are well equipped to teach password practices to their children and model good practices themselves. Results from this study suggest there are several areas where cybersecurity researchers and practitioners can support parents.

First, there is a need for guidance on effective password creation and maintenance strategies for parents. Guidance should be both practical and usable given the large number of devices, accounts, and personal passwords parents have and given parents' prioritization and practice of creating and maintaining usable passwords. For example, 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 [7]. It will be helpful to provide guidance to parents and youth on how to evaluate what they want to protect, how strong a password is needed, and how to create an appropriate password. Relatedly, researchers and practitioners should promote effective tools to help parents create and track their passwords. Tools such as password generators and password managers may help parents to achieve their goals of creating strong passwords that are easy to remember and use. However, our results suggest few parents use these tools and are aware they exist. Therefore, increased awareness and communication on benefits of such tools are needed.

Second, parents need guidance on effectively teaching password creation and maintenance to their children. Guidance must consider age-appropriate strategies for teaching password practices, as well as assist parents in modifying teaching password practices as children age. Finally, researchers and practitioners should increase outreach to provide resources and best practices to parents.

6   Limitations

Our study has few limitations that are common to many usable security studies. First, results of this study are specific to the parent sample from a panel who self-selected to participate. Thus, our results may not generalize to the broader parent population. Second, the survey gathered parents' self-reported password practices. Parents' actual password behaviors were not measured and may differ from the behaviors reported. Although measuring parents' actual behaviors is an important area for future study, the value of self-reported data should not be minimized, as it can be vital for obtaining insight into the mental models that drive human behavior. Third, like many other studies of password behavior, to prevent privacy concerns of asking for passwords with an authentic scenario, we asked parents to generate hypothetical passwords. Using a hypothetical password scenario constrains our ability to understand genuine password behavior and to gain a nuanced understanding about parents' contextually specific password behavior.

7   Conclusion

This study focused specifically on parents in order to understand their password behaviors and involvement with their children's password practices. Not surprisingly, we found that parents' password practices do not differ much from password practices of typical adults which include parents and non-parents; parents in our study understand the importance of creating strong and usable passwords, but may struggle to practically implement these priorities, as parents also tend to have many personal passwords. We gain important insight on that parents are actively involved in their children's password behaviors, especially helping elementary school children create and maintain their passwords. Cybersecurity researchers and practitioners can help parents by providing guidance, tools, and outreach to successfully support both parents' own password practices as well as with teaching their children to establish good password practices.

There are several areas for future work. First, research should explore parents' involvement over time as children age. Longitudinal research may be able to identify

how and when gradual release of parental involvement in children's password practices occurs. Second, research is also needed to understand dynamic and bidirectional influences between parents and children within the same family. While the current study focused on parents' experiences with the first child they reported in the survey, future work should examine the experiences of parents and children together, as well as understand the influence and role of family members, such as siblings. Third, additional research is also encouraged to examine the role of influences outside the family such as schools, educators, and peers on children's password understanding and practices.

References

1. Abraham, M., Crabb, M., Radomirović, S.: "I'm doing the best I Can": understanding technology literate older adults' account management strategies. In: Parkin, S., Viganò, L. (eds.) STAST 2021. LNCS, vol. 13176, pp. 86–107. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-10183-0_5

2. Agresti, A.: An Introduction to Categorical Data Analysis, 3rd edn. Wiley, Hoboken (2018)

3. Bandura, A., Walters, R.H.: Social Learning Theory, vol. 1. Prentice Hall, Englewood Cliffs (1977)

4. Choong, Y.-Y., Theofanos, M.F., Renaud, K., Prior, S.: Passwords protect my stuff"—a study of children's password practices. J. Cybersecur. **5**(1), 19, Article no. tyz015 (2019). https://doi.org/10.1093/cybsec/tyz015

5. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.F.: The tangled web of password reuse. In: NDSS 2014, vol. 2014, pp. 23–26 (2014). 15 pages

6. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657–666 (2007)

7. Grassi, P.A., et al.: Digital identity guidelines: authentication and lifecycle management. Technical Report 800-63B, NIST Special Publication (2017). https://doi.org/10.6028/NIST.SP.800-63b

8. Hernández-Alava, M., Popli, G.: Children's development and parental input: evidence from the UK millennium cohort study. Demography **54**(2), 485–511 (2017). https://doi.org/10.1007/s13524-017-0554-6

9. Inglesant, P.G., Angela Sasse, M.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 383–392 (2010). https://doi.org/10.1145/1753326.1753384

10. Kawu, A.A., Orji, R., Awal, A., Gana, U.: Personality, culture and password behavior: a relationship study. In: Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities, pp. 1–4, Article no. 36 (2018). https://doi.org/10.1145/3283458.3283530

11. Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L., Vitak, J.: "No telling passcodes out because they're private" understanding children's mental models of privacy and security online. Proc. ACM Hum.-Comput. Interact. **1**, CSCW, 1–21, Article no. 64 (2017). https://doi.org/10.1145/3134699

12. Lamichhane, D.R., Read, J.C.: Investigating children's passwords using a game-based survey. In: Proceedings of the 2017 Conference on Interaction Design and Children, pp. 617–622 (2017). https://doi.org/10.1145/3078072.3084333

13. Livingstone, S., Helsper, E.J.: Parental mediation of children's internet use. J. Broadcast. Electron. Media **52**(2), 581–599 (2008). https://doi.org/10.1080/08838150802437396

14. Maqsood, S., Biddle, R., Maqsood, S., Chiasson, S.: An exploratory study of children's online password behaviours. In: Proceedings of the 17th ACM Conference on Interaction Design and Children, pp. 539–544 (2018). https://doi.org/10.1145/3202185.3210772

15. Mayer, P., Volkamer, M.: Addressing misconceptions about password security effectively. In: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, pp. 16–27 (2018). https://doi.org/10.1145/3167996.3167998

16. Morris, R., Thompson, K.: Password security: a case history. Commun. ACM **22**(11), 594–597 (1979). https://doi.org/10.1145/359168.359172

17. Pearman, S., et al.: 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, pp. 295–310 (2017). https://doi.org/10.1145/3133956.3133973

18. Pearman, S., Zhang, S.A., Bauer, L., Christin, N., Cranor, L.F.: Why people (don't) use password managers effectively. In: 15th Symposium on Usable Privacy and Security (SOUPS 2019), pp. 319–338 (2019)

19. Ratakonda, D.K., French, T., Fails, J.A.: My name is my password: understanding children's authentication practices. In: Proceedings of the 18th ACM International Conference on Interaction Design and Children, pp. 501–507 (2019). https://doi.org/10.1145/3311927.3325327

20. Rideout, V., Robb, M.B.: The Common Sense Census: Media use by tweens and teens. Common Sense Media 2019 census full report. Common Sense Media. San Francisco (2019). https://www.commonsensemedia.org/sites/default/files/research/report/2019-census-8-to-18-full-report-updated.pdf

21. Rim, K., Choi, S.: Analysis of password generation types in teenagers–focusing on the students of Jeollanam-do. Int. J. u-and e-Serv. Sci. Technol. **8**(9), 371–380 (2015)

22. Sharpe, D.: Chi-square test is statistically significant: now what? Pract. Assess. Res. Eval. **20**(1), Article no. 8 (2015). https://doi.org/10.7275/tbfa-x148

23. Smahel, D., et al.: EU Kids Online 2020: Survey results from 19 countries. EU Kids Online, London (2020). http://hdl.handle.net/20.500.12162/5299

24. Tobert, E.S., Biddle, R.: The password life cycle: user behaviour in managing passwords. In: 10th Symposium on Usable Privacy and Security (SOUPS 2014), pp. 243–255 (2014)

25. Tam, L., Glassman, M., Vandenwauver, M.: The psychology of password management: a tradeoff between security and convenience. Behav. Inf. Technol. **29**(3), 233–244 (2010). https://doi.org/10.1080/01449290903121386

26. Taneski, V., Heričko, M., Brumen, B.: Password security—no change in 35 years? In: 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1360–1365. IEEE (2014). https://doi.org/10.1109/MIPRO.2014.6859779

27. Theofanos, M., Choong, Y.-Y., Murphy, O.: "Passwords keep me safe"–understanding what children think about passwords. In: 30th USENIX Security Symposium (USENIX Security 2021), pp. 19–35 (2021)

28. Ur, B., et al.: "I added '!' at the end to make it secure": observing password creation in the lab. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), pp. 123–140 (2015)

29. Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F.: Do users' perceptions of password security match reality? In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 3748–3760 (2016). https://doi.org/10.1145/2858036.2858546

30. Walia, K.S., Shenoy, S., Cheng, Y.: An empirical analysis on the usability and security of passwords. In: 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), vol. 1, no. 7, pp. 1–8. IEEE (2020). https://doi.org/10.1109/IRI49571.2020.00009

31. Wang, C., Jan, S.T.K., Hu, H., Bossart, D., Wang, G.: The next domino to fall: empirical analysis of user passwords across online services. In: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, pp. 196–203 (2018). https://doi.org/10.1145/3176258.3176332

32. Wash, R., Rader, E., Berman, R., Wellmer, Z.: Understanding password choices: how frequently entered passwords are re-used across websites. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pp. 175–188 (2016)

33. Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., Chiasson, S.: From nosy little brothers to stranger-danger: children and parents' perception of mobile threats. In: Proceedings of the 15th International Conference on Interaction Design and Children, pp. 388–399 (2016). https://doi.org/10.1145/2930674.2930716

34. Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., Schaub, F.: Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–15 (2020). https://doi.org/10.1145/3313831.3376570