An Exploratory Study of Children's Online Password Behaviours

Sumbal Maqsood
Carleton University
Ottawa, Canada
sumbal.maqsood@carleton.ca

Sana Maqsood
Carleton University
Ottawa, Canada
sana.maqsood@carleton.ca

Robert Biddle
Carleton University
Ottawa, Canada
robert.biddle@carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

IDC '18, June 19–22, 2018, Trondheim, Norway
© 2018 Association for Computing Machinery.
ACM 978-1-4503-5152-2/18/06... $15.00.
https://doi.org/10.1145/3202185.3210772

Abstract

With increasing use of technology and the Internet among children, we explore how they create passwords to protect their personal information. We conducted a study with children 11 to 13 years to understand their password practices. The results of the study indicated that these children create simple passwords consisting of their personal information, believe that these passwords are hard for a stranger to guess and do not have good understanding of creating strong passwords.

Author Keywords

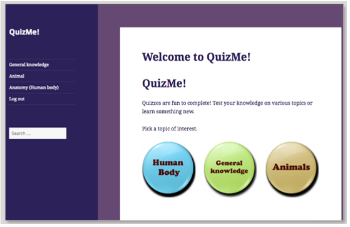
Children's security, Password design, Usable security, Authentication

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction

Children's access to the Internet has steadily increased over the years. Globally, one-third of Internet users are children[3]. Children younger than 15 years are online as often as adults[7] from home and school, often using their mobile devices[3]. On a daily basis, they interact with different websites and applications to learn, socialize and engage in issues that matter to them. These websites often require



Welcome to QuizMe!

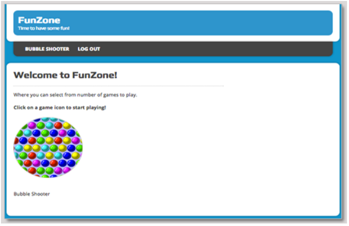
QuizMe!

Quizzes are fun to complete! Test your knowledge on various topics or learn something new.

Pick a topic of interest.

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

Task: complete a quiz



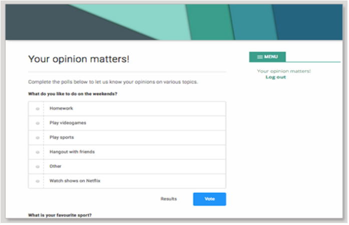
Welcome to FunZone!

Where you can select from number of games to play.

Click on a game icon to start playing!

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

Task: play a game



Your opinion matters!

Complete the polls below to let us know your opinions on various topics.

What do you like to do on the weekends?

- ○ Homework
- ○ Play videogames
- ○ Play sports
- ○ Hangout with friends
- ○ Other
- ○ Watch shows on Netflix

What is your favourite sport?

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

Task: complete a poll

creating an account involving children's or parents' personal information. Children are often unaware of threats to which they are exposed. Parents are concerned about their children's safety and they extensively monitor children's activities, even at the expense of breaching their privacy and trust[11]. This, however, does not help teach children how to create secure passwords nor teach how to manage their own data.

Generally, children have incomplete mental models of privacy and how to protect their personal information[8]. As a result, they place themselves at risk because they do not understand the implications of their behavior. Insecure password practices could put increase risks of various online threats. Currently, there is sparse research on how children authenticate and protect themselves online. Research has shown that children often forget their passwords and engage in poor password management strategies[9, 6]. In this study, we looked at the *types* of passwords children create and to further understand their password practices.

Related research

Text-based passwords are commonly used for authentication[1] despite their usability and security problems[5]. Even adult users often have difficulty creating passwords that are secure and memorable[12]. Bonneau et at al.[2] compared authentication schemes to replace passwords. They found that all authentication schemes have drawbacks, suggesting that passwords will remain a primary means of authentication for the foreseeable future. As a result, children regularly interact with systems that use text-based passwords.

Read at al.[9] found that children have a basic understanding of passwords. They found that children believed that passwords are used to stop people from getting access to their information. In their study, they found that children created simple passwords consisting of whole words. Simplicity was calculated based on the number of characters used and the number of whole words used in the passwords. They did not look further at the composition of the passwords. Lamichhane at al.[6] looked at composition of children's password. They found that most children created password with their personal information and have trouble recalling long and complex passwords compared to simple ones. However, in their study, children created passwords with no password policy in place. In real life, websites and applications enforce various password policies that impact users' password creation strategies. We are interested in finding out how children create passwords given different password rules.

Other related work has compared children's ability to use graphical passwords compared to text passwords [4]. They found graphical passwords were more memorable in the short-term, but not necessarily in the longer-term, compared to text-based passwords.

Study

The study was conducted with 20 children participants between ages 11 to 13 years. 11 participants were female and 9 were male. Ten participants were 11 years old, six were 12 years old and four were 13 years old. Participants were regular Internet users. Most participants (75%) logged into an application or a website at least once a day and the remaining 25%, logged in at least weekly.

Procedure

Parents read and signed the consent form. They did this apart from their child since it contained information about the study that the child should not know until the study was finished. Once the consent form was signed, the researcher read the assent form to the child participant. Par-

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

Table 1: Password creation rules.

ticipants were told that they were testing usability of three websites. We believed that if participants knew that we were interested in studying their password behaviour, they might be more careful in the type of passwords they create. The three websites we created were: "QuizMe", "FunZone","OpinionMatters" (as shown in Figure 1, Figure 2 and Figure 3). Each website had different password creation rules that varied in complexity (Table 1). Latin square design was used for presentation order of the websites to minimize ordering effects. A username was provided to the participants at the beginning of the session. The same username was used for registering on all three websites.

Participants first completed a demographic questionnaire and then interacted with each of the three websites. On each website, they created an account, logged in, completed a task (quiz, poll, games), logged out of the site and answered a brief interview. This interview asked their thoughts about the website and their password creation strategy. This cycle repeated for all three websites, after which participants completed a post-test questionnaire about their overall experience. Finally, participants were asked to login to each of the three websites.

Results and discussion

We looked at participants' password creation times, login time, recall, the types of passwords they created, and password strength.

Creation time

Participants took longer (M=82.05, SD=32.27) to create passwords in the *high complexity* condition than *medium complexity* (M=36.40, SD=39.63) or *low complexity* (M=54.10, SD=15.94) conditions (as shown in Figure 4). A significant difference was seen in creation time between the three conditions, F(2,38) = 16.54, $p<.05$.

Therefore, password creation time increased the complexity of the password policy. Based on the Latin Square ordering, 7 participants first created a high complexity password, 7 participants first created a medium complexity password and 6 participants first created a low complexity password. The order in which the three conditions were presented to the participant did not affect their average password creation time (across the three conditions), F(2,17)=3.02, p=0.08.

Login time

Participants had to login twice to each website. They first logged in after creating each password and then again at the end of the study. As shown in Figure 5, it took participants slightly longer to login during the second login

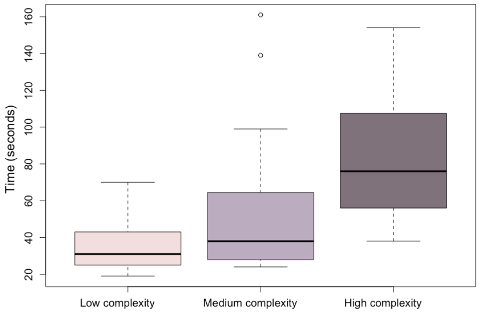


Figure 4: Boxplot of time in seconds it took participants to create passwords in each of the three conditions

attempt. However, we found no significant difference in login time between the three conditions, F(1.69,32.03) = 2.54, p=0.10. Also, there was no significant difference in login time between the two login attempts, (F(1,19)=2.30, p=.15). This is mostly likely because participants immediately logged into the website after creating the password, so there was no significant time lapse between the first and second login.

Recall

12 participants successfully logged in during both login attempts without any failures. However, 8 participants had difficulty recalling their password during the first or the second login attempt. In most failures, the password entered by the participant was closely related to their actual password. Therefore, it seems plausible that participants did not forget their password, but instead made errors in entering it.

Password composition

From the questionnaires, we found that 55% of participants used their personal information to create the passwords. They most likely did this to make it easier for them to remember the passwords. 14 participants reported that they used their actual password (N=4) or parts of their actual password (N=10). Participants used the exact same password (N=7) in at least two conditions or had similarity in their passwords across conditions (N=13). Participants found it most difficult to create passwords in the *high complexity* condition due to the number of rules (as shown in Figure 6). Participants created similar passwords in the *low* and *medium* complexity conditions even though the *low* complexity condition had fewer rules. We found that even with minimal password rules, participants created passwords that included uppercase characters, lowercase characters or numbers. This is most likely because participants are very familiar with the rules used in the *medium complexity* condition from their previous real life experiences. 50% of participants had difficulty understanding the special character rule. Mostly, it was younger participants (11 and

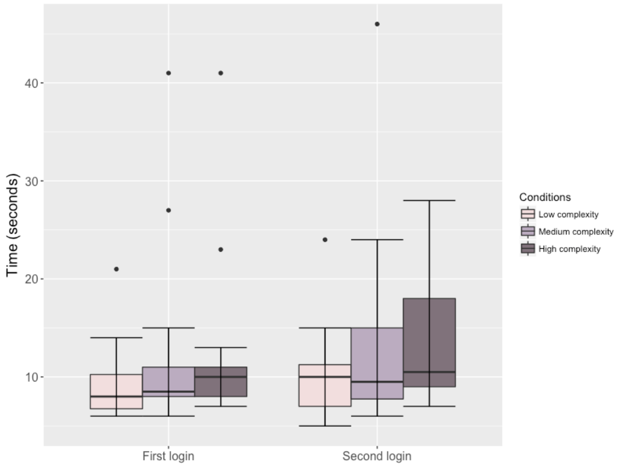


Figure 5: Login time of first and second login attempts in each of three conditions

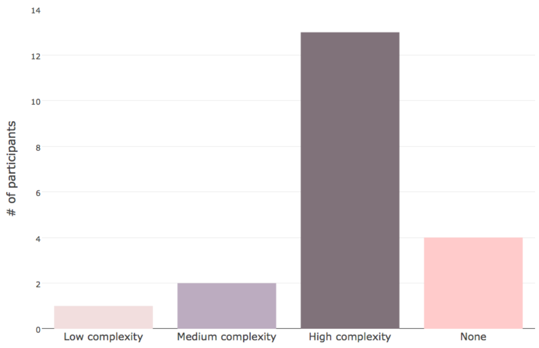


Figure 6: Condition in which participants found it most difficult to create the password

12 years old)who had difficulty with this rule.

Password strength

Most participants reported that the passwords they created would be hard for a stranger to guess. Among those who were less confident in their password, participants believed that their passwords were too simple and contained their personal information, such as name or age. Participants were concerned about their privacy. Specifically, they did not want anyone especially their siblings to have access to their account. To assess password strength, we calculated the entropy of passwords using Shannon's entropy formula[10]. There was no significant difference in password entropy between the three conditions, F(1.26,29.93)=.32, p=0.63. However, entropy does not take into account dictionary attacks, commonly used words, or pattern of characters in a password. Due to this, we used the NIST guidelines to subjectively assess passwords on scale of 1 (least secure) to 5 (highly secure). We looked at password's length, complexity, vulnerability to dictionary attack, inclusion of commonly used words, and use of repetitive/sequential characters (e.g, "123"). Two researchers independently scored each of the passwords in the three conditions. A weighted Cohen's Kappa(κ) test showed moderate agreement between the two researchers' ratings (k=0.54, p $<$.01). Most passwords scored between 1 to 3, suggesting overconfidence when participants thought that they created secure passwords. There was a significant difference in password strength between the three conditions (F(2,38)=20.45, p$<$.01). Pairwise post hoc tests using Tukey HSD correction showed that password strength significantly differed between all three conditions (p$<$.01).

Conclusion and limitations

We found that children create simple passwords containing their personal information. However, they believe that these passwords would be hard for a stranger to guess. This suggests that children have flawed understanding of what constitutes a strong password and that more targeted instruction at a young age could help them better protect themselves online. As well, we suspect that children are learning to create simple and weak passwords from their parents/guardians. Further studies with parents could explore their knowledge of secure passwords and what they teach their children about the topic.

Most of the children created relatively long passwords that included uppercase characters, lowercase characters, or numbers. The average length of a password across the three conditions was nine, indicating that children are used to creating passwords longer than the six characters required in this study. However, they might have difficulty remembering long and complex passwords that do not contain their personal information. Therefore, we suggest that password policies designed for children of ages 11 to 13 could safely include mixed character case, numbers, and a length of at least eight characters. Special characters should only be included if children are first taught this terminology. In our study, once the special character rule was explained, children quickly understood its meaning. Further studies need to be conducted to better understand what terminology would make password rules easier for children to understand. The main limitations of our study were the duration of the study for testing password memorability and the ecological validity. In real life, children most likely do not create passwords one after another in such a short time frame. As well, we provided guidelines but relied on researchers to make an assessment of password strength. Although different factors are taken into account when making the assessment, it is subjective. Further research could explore the long-term memorability of password created using different password policies and develop a strength measure that more adequately considers different factors of what makes a password strong. We also need strategies to teach children how to create secure passwords, and password policy guidelines for children of various age groups.

REFERENCES

1. M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi. 2008. Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. In *2008 Second Asia International Conference on Modelling; Simulation (AMS)*.

2. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society.

3. Jasmina Byrne, Daniel Kardefelt-Winther, Sonia Livingstone, and Mariya Stoilova. 2016. Global Kids Online: research synthesis 2015-2016. (2016).

4. Jasper Cole, Greg Walsh, and Zach Pease. 2017. Click to Enter: Comparing Graphical and Textual Passwords for Children. In *Proceedings of the 2017 Conference on IDC*. New York, NY, USA.

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

6. Dev Raj Lamichhane and Janet C. Read. 2017. Investigating Children's Passwords Using a Game-based Survey. In *Proceedings of the 2017 Conference on IDC*. ACM, New York, NY, USA.

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

8. Janet C. Read and Russell Beale. 2009. Under My Pillow: Designing Security for Children's Special Things. In *Proceedings of the 23rd BCS-HCI (BCS-HCI '09)*. Swinton, UK.

9. Janet C. Read and Brendan Cassidy. 2012. Designing Textual Password Systems for Children. In *Proceedings of the 11th IDC*. ACM.

10. Claude E Shannon. 2001. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review* 5, 1 (2001).

11. Valerie Stevens. 2012. Young Canadians in a Wired World. Phase III. Talking to Youth and Parents about Life Online. (2012).

12. J. Yan, A. Blackwell, R. Anderson, and A. Grant. 2004. Password memorability and security: empirical results. *IEEE Security Privacy* (2004).