Cyberheroes: The Design and Evaluation of an Interactive Ebook to Educate Children about Online Privacy[☆]

Leah Zhang-Kennedy[a,*], Yomna Abdelaziz[b], Sonia Chiasson[c]

School of Computer Science, Carleton University, Canada

[a] *leah.zhang@carleton.ca*
[b] *YomnaAbdelaziz@cmail.carleton.ca*
[c] *chiasson@scs.carleton.ca*

Abstract

We designed an educational interactive ebook called Cyberheroes and evaluated it to assess its effectiveness at increasing children's online privacy knowledge and behaviour, and supporting child-parent privacy-related discussions. We conducted a user study with 22 children (aged 7 to 9) and 22 parents that included usability evaluations and privacy knowledge and behaviour assessments with children pre/post-reading and 1-week later. Cyberheroes considerably increased children's online privacy knowledge and reported privacy behaviour, and led to superior 1-week knowledge retention compared to the text-only control. Furthermore, Cyberheroes facilitated longer child-parent privacy discussions during co-reading than the control. Children and parents found Cyberheroes engaging, easy to use, and easy to learn. We discuss our interactive ebook's role in children's acquisition, retention, and transfer of knowledge, and the role that interactivity, previous knowledge, and parental guidance play in children's online privacy education.

Keywords: Privacy Education, Interactive Ebook, Mobile Learning, Prototyping, User Study, Children

[☆]This research expands preliminary work published as an extended abstract: "Teaching with an Interactive Ebook to Improve Children's Online Privacy Knowledge", presented at Interaction Design and Children (IDC), ACM, 2016.

*Corresponding author.

Authors' copy (version: February 8, 2017). To appear in *International Journal of Child-Computer Interaction*. DOI: 10.1016/j.ijcci.2017.05.001

1. Introduction

Access to mobile media devices has increased dramatically among young children, with 96.6% of 6-month to 4-year-olds using mobile devices on a daily basis [1]. Frequent online access increases children's exposure to online privacy risks [1]. Child-friendly education initiatives are needed to empower children to be secure and responsible digital citizens [2, 3].

While many privacy education initiatives focus on tweens, teens, and adults as their primary audience, we lack appropriate resources to teach young children, who are still developing literacy and cognitive skills, and have limited experience. These limitations pose constraints on educational content and format.

We propose that security and privacy information presented creatively as an interactive ebook could be made engaging, comprehensible, and memorable for children due to the media's positive learning effects, such as improved language and literacy skills [4], increased engagement [5], support for personalized learning [6], and support for learning by adult instruction [7].

We designed an interactive ebook called Cyberheroes (Screenshots in Figure 1). A user study assesses whether it is successful as a learning facilitator, and whether it is an effective format for improving the privacy knowledge and behaviour of children 7 to 9 years old (grades 1 to 3 in North America). Children of this age group have developed moderate literacy, memory, and cognitive abilities [8] that enable them to engage more reliably in research studies [9].

The primary contributions of our study are the design and prototyping of privacy education material specifically for young children based on instructional design principles, and to the best of our knowledge, the first empirical evaluation of a privacy education tool in showing significant learning effects on children's privacy proficiency determined based on assessments of knowledge and behaviour pre-test, post-test, and 1-week after reading the interactive ebook compared to a text-only control. We discuss the implications of our findings on children's online privacy education.

2. Related Work

We define children's interactive (or enhanced) ebooks as digital books with multimodal enhancements such as sound, animation, and narration. Interactive ebooks have the potential to change the way children read and consume content because of their interactivity and convenience [10]. While several works found that multimedia enrichments had positive effects on children's user experience [11], comprehension of the story content [12, 13, 4], narrative inference [14], and language skills [14, 4], others cautioned that multimedia features could distract children from reading [15] and hinder comprehension [16, 17].

Several design guidelines were proposed. Korat and Shamir [18] argued that multimedia features should be strategically used to support children's attention. Dünser and Hornecker [19] advised that interactive sequences should augment and illustrate the text, advance the story, and provide clear signals when the interaction is triggered. Roskos et al. [20] highlighted the distinguishing features of three research-based analytic tools (de Jong-Bus Tool, Clark-Mayer Tool, Blueprint Key Tool) for evaluating interactive ebooks. Schugar et al. [10] suggested that important considerations are vocabulary/inference support, ratio of supporting and extending interactions to distracting interactions, time required to engage in interactions, and frequency/placement of interactions.

Designing security and privacy educational tools has several unique challenges. First, persuading children to behave in a privacy-preserving manner is difficult because, like adults, they typically do not regard privacy and security as primary concerns [21]. A tradeoff often exists and users may not be motivated to invest time on security and privacy [22]. Second, attackers will exploit any information leaked or extracted online and actively try to trick legitimate users, making it difficult to provide users with some types of helpful advice. For example, advice that guides users toward secure actions may also help attackers to circumvent it. Third, unlike other safety advice that remains relatively static over time, such as wearing a seatbelt, security and privacy threats constantly change and evolve, making it difficult to give users concrete protective advice.

Fourth, users typically have poor mental models[1] of security threats [24, 25], which could have negative consequences on their protection behaviour. Security and privacy education tools therefore, should aim to teach children critical-thinking about the consequences of their online actions [2], improve their mental models [26], and influence their behaviour [3].

3. Design of Cyberheroes

Cyberheroes[2] is an educational interactive ebook about online privacy designed for children under the age of 10. Four screens are shown in Figure 1. The central story is that Cyberheroes (a play on superheroes) must maintain their secret identities on the Internet. Due to the popularity of the superhero genre through comics and film, we believed the story would resonate with children and make the concept of privacy easy to understand. The story spans across 13 interactive screens and centres around two Cyberheroes, Ally and Bobby, who lost their cyberpowers and must face the consequences. Each cyberpower is a privacy-related lesson about personal information, online chatting, location sharing, cyberbullying, and passwords (summarized in Figure 1D).

Druin [27] classified children's roles in the design process as *users*, *testers*, *informants*, or *partners*. To inform the design of Cyberheroes, we first identified gaps in children's privacy conceptions, where 14 children and their parents participated as *informants* in an interview study [26]. We found children's conception of online privacy is based on their understanding of physical privacy and safety, and their perceived online threats are different than the threats parents perceived to be faced by children [26]. Next, we incorporated these findings into our ebook design, where we leveraged physical privacy concepts and focused on risks that are relevant to children. Our first design goal was to help children develop skills in protecting their online privacy, which is assessed by testing

[1] A *mental model* is a simplified internal concept of how something works in the real world [23].

[2] The Cyberheroes interactive ebook app is available for free online at `http:/www.versipass.com/edusec/cyberheroes` and in the App Store (for iPads).

Figure 1: Sample screens and interactions from Cyberheroes. A) Home Screen: the user presses the "play" button to start playing; B) Online Chatting: the user taps on the characters on screen to reveal their real identity; C) Digital Trail: the user drags the pink eraser over the digital trail to "erase" it, then the trail reappears; D) Cyberpowers: the user taps on each character to transform them into Cyberheroes.

those skills before, after, and one week after using the interactive ebook. Our second design goal was to create an educational tool that is engaging, easy to use, and easy to learn for children, which is assessed by a usability evaluation. In meeting these goals, children acted as *users* and *testers* in our research at the end of the design process.

We wrote the Cyberheroes story and created pencil sketches and storyboards for the narrative. The character design and storyboards were refined after receiving feedback from members of our lab, other graphic designers, and elemen-

ID Principles	Key Features
Multimedia	Use words and graphics rather than words alone.
Contiguity	Align words to corresponding graphics.
Redundancy	Explain visuals with words in audio or text, but not both.
Coherence	Avoid extraneous audio, graphics, and words.
Personalization	Use conversational (child-friendly) language.
Segmenting	Managing complexity by breaking a lesson into parts.

Table 1: Instructional design principles for e-learning by Clark & Mayer [28]

tary school teachers. The finalized illustrations were created by us in Adobe Illustrator using a Wacom graphics tablet. Some royalty-free stock images were adapted for the backgrounds. The interactive ebook was implemented using GameSalad Creator[3].

Design guidelines for children's technology follow general HCI design guidelines for adults (e.g., [29, 30, 31]), but have three interrelated high-level requirements: perceivability, operability, and developmental fit [32]. First, it should be easy to perceive by children what they can do with the technology, and what the technology is currently doing [32]. This can be accomplished by simplifying the user interface to account for children's developmental needs [32], speaking in a child-friendly language (e.g., written, visual, auditory) [32], creating intuitive visual mappings [29] to match what children want to accomplish, and using recognition over recall techniques to support memory [31]. Second, a user interface should be easily operated by children given their physical and motor limitations [32]. As such, real or virtual objects need appropriate affordances and constraints to avoid undesirable errors [29]. Third, the user interface should meet children's abilities and experience in understanding how to use a technology [32]. It can be achieved by enabling children to quickly perceive the consequences of their interactions and undo the action if necessary [30]. Fur-

[3]GameSalad Creator is a developer tool kit for making interactive games.

thermore, sociocultural views on children's development [33] advocate that the design of children's technologies should support social use with peers, caregivers, and teachers.

Cyberheroes applies instructional design principles for e-learning [28] (summarized in Table 1.) to addresses the requirements of perceivability, operability, and developmental fit of our target age group.

3.1. Perceivability

The lesson content in Cyberheroes is simplified by using the *Segmenting* principle, where individual screens address no more than one point or topic. The simple interface requires only tapping and dragging. Interactive objects that enable tapping are visually mapped with a rotating star and draggable objects are visually mapped with a directional pulsing hand symbol (Figure 1C). Since children rely on concepts from their their physical environment to understand online privacy [26], we used physical security metaphors to communicate abstract online concepts where appropriate. For example, passwords in the interactive ebook protect a vault that contains Ally and Bobby's favourite toys. We used the *Personalization* principle to give advice in child-friendly language and speaking directly to the reader (e.g., "be careful of who *you* trust online").

3.2. Operability

The interactive ebook is optimized for high-resolution retina iPad screens to ensure a large reading surface. All visual interactive objects are large to facilitate selection. To help readability, certain words are enlarged to emphasize their importance. All interactive elements are visually marked to make them easily distinguishable from the non-interactive elements. Based on the *Redundancy* principle, we designed the interactive ebook with no voice narration, as research shows that explaining text with audio could hurt learning [28]. The interactive ebook has a "mute all sounds" option to silence sound effects and background music to support individuals' reading preferences. Interactive features are designed to show cause and effect relationships, advance the story,

or to infer moods and feelings of the characters or the situation. Extraneous content is avoided to support the *Coherence* principle.

3.3. Developmental Fit

Based on the *Multimedia* principle, we created illustrations that are congruent with the instructional message. We filled each page with colourful illustrations and minimize textual instruction to account for children's limited vocabulary and to stimulate the imagination of our target age group. Text in the interactive ebook is given careful typographic consideration to ensure that it works with the illustrations to support the *Contiguity* principle. Children's interaction with the interface shows immediate cause and effect relationships and consequences of the characters' actions. For example, the "online trust" page (Figure 1B) shows that some people online are not who they say they are. When the user taps on the top right character, the image of 9-year-old "Alex" changes to 42-year-old "Mr. R". Ally responds to the change with a surprised expression and a shriek. On the "digital trail" page (Figure 1C), the trail fades away when the user attempts to "erase" it by dragging the pink eraser, but it always reappears, illustrating the difficulty with removing online content once posted. Cyberheroes supports parental instruction. A "For Parents" link on the main screen teaches parents how to use the interactive ebook with their children to engage them in privacy-related conversations.

4. Methodology

In our between-subject study, the dependent variable is *privacy proficiency* measured based on children's privacy knowledge and behaviour, and the independent variable is the type of media (i.e. the Cyberheroes interactive ebook and a text-only version of the same narrative as the control). Pairs were pseudo-randomly assigned to follow either the *ebook* or the *text* group procedure outlined in Table 2.

The experiment took two sessions conducted a week apart and lasting approximately 40 minutes for session 1 and 15 minutes for session 2. The depen-

dent variables were measured pre-reading (Pre-Test), post-reading (Post-Test), and a third time 1-week post-reading (1-week-Test). The *ebook* group was provided with 2 iPads and the *text* group was provided with 2 letter-sized printouts. Both groups were given full control of the co-reading sessions.

4.1. Participants and Recruitment

The sample included 22 child-parent dyads with 14 girls and 8 boys between the ages of 7 to 9 (Mean = 8). To minimize the effects of gender differences, the sample is balanced with seven girls and four boys per group. Children's mean age is 8.1 years in the *ebook* group and 7.9 years in the *text* group. Participation was restricted to one child per family who used a mobile device regularly. None of the children had prior formal privacy education. Nineteen mothers and three fathers accompanied the children. The parents were between the ages of 30 to 44 and from a wide range of socio-economic backgrounds and education levels.

After receiving clearance from our institution's ethics board, invitations were shared with parents in the cities of Kitchener-Waterloo and Cambridge, ON., Canada through public parenting groups on social media and email.

The adult participants signed informed consent forms for their own and their child's participation. The child participants provided verbal assent. Each family received a $20 honorarium. The participants were anonymized by codenames using the letter "P" for parent and "C" for child, an identification number (1 – 11 per condition), and the condition they participated in (*ebook* or *text*). For analysis purposes, the child-parent dyads were coded in such a way that the pair can still be matched (e.g., C1-ebook is the child of P1-ebook).

4.2. Evaluation Measures

A) Demographic/Activities, Pre-Evaluation Questionnaires: All 22 parents completed an Adult Demographic Questionnaire (age, gender, education, occupation). They completed a Child Demographic & Activities Questionnaire for their children. The demographic portion contained children's age, gender, and grade. The activities portion asked about children's daily device use, the types

Procedure & Materials			
Ses.	**Sub.**	**Ebook Procedure**	**Text Procedure**
1	Parent	A) Demographic/Activities	A) Demographic/Activities
	Child	B) Pre-Test	B) Pre-Test
	Parent-Child	Co-read interactive *ebook*	Co-read narrative *text*
	Parent	C) Adult Usability	N/A
	Child	C) Child Usability	
		B) Post-Test	B) Post-Test
1-week Interval			
2	Child	B) 1-Week-Test	B) 1-Week-Test
	Parent-Child	N/A	Co-read interactive *ebook*
	Parent		C) Adult Usability
	Child		C) Child Usability

Table 2: Summary of the study procedure. Questionnaires – A & C; Interviews – B. Materials are described in Section 4.2. Corresponding colours represent similar activities.

of devices used, and online activities. Lastly, we inquired whether children had prior experience reading interactive e-books and privacy education.

In the Pre-Evaluation Questionnaire, all parents sorted and ranked the importance (rank 1 = most important; rank 5 = least important) of "fun", "age-appropriateness", "ease of use", "effectiveness", and "educational value" for choosing educational apps for kids. The questionnaire was intended to assess whether there is a dominant criteria for parents.

B) Children's Privacy Proficiency Tests: We designed each privacy proficiency test to contain four knowledge-based questions and six behaviour-based questions assessing children's overall proficiency to practice privacy-conscious behaviour. Our knowledge-based questions inquired about children's understanding of privacy and personal information (e.g., what it is, how to protect it, what could happen if people had no privacy). To test children's behaviour, they responded to situation-based scenarios on the topics of personal information, online chatting, location sharing, cyber-bullying, passwords, and digital trail. Children responded to each scenario by explaining what they would do

and why. For example, the pre-test scenario for passwords is: *Your best friend wants to borrow your password to email a funny picture to a friend that you both know. What would you do? Why?* The pre-tests established a baseline for each child, and the questions were repeated verbatim in the post-tests. The 1-week-tests evaluated the same concepts but contained alternate scenarios. The tests were administered as interviews, which is an appropriate data collection method for children 7 years and older that has several benefits over surveys, including reducing fatigue, increasing attention, and enabling the researcher to prompt children for further information if the answers are unclear or vague [34]. Our interviews with children were audio recorded and transcribed.

C) Child & Parent Usability Questionnaires: The child questionnaire contained eight questions. We first measured engagement using an Again-Again Table [35] asking: *1) Would you read Cyberheroes again?*. Next, children answered five questions using the 5-point Smileyometer [35] (i.e., visual Likert-scales): *2) How fun was the Cyberheroes ebook? 3) How easy was it to use the Cyberheroes ebook? 4) How well did you learn from the Cyberheroes ebook? 5) How likeable were Ally and Bobby? 6) How willing would you be to show the Cyberheroes ebook to other kids?* In the analysis, the Again-Again Table evaluations were coded as 3 for "yes", 2 for "maybe" and 1 for "no". The Likert-scale questions were coded from 1 for least positive, to 5 for most positive. Lastly, children answered two open-end questions: *7) What did you like about the Cyberheroes ebook? 8) What did you dislike about the Cyberheroes ebook?*

The questionnaire for parents contained twelve questions. Questions 2, 3, 7, and 8 were reused from the Child Usability Evaluation. The remaining Likert questions were: *1) How effective was the Cyberheroes ebook as a learning tool for children. 2) How age-appropriate was the Cyberheroes ebook? 3) How educational was the Cyberheroes ebook? 4) How willing would you be to read the Cyberheroes ebook again with your child? 5) How willing would you be to use the Cyberheroes ebook to teach your child about privacy? 6) How well did you and your child interact with Cyberheroes? 7) How well did Cyberheroes facilitate conversations about privacy between you and your child?* Lastly, an open-ended

question asked: *8) What would you add or change to Cyberheroes?*

We wanted make the study experience fun for families and give both the *text* and *ebook* groups the opportunity to view and evaluate Cyberheroes. The usability evaluation procedure is designed to not confound the results of children's privacy proficiency tests. Both the *text* and *ebook* conditions completed the privacy proficiency tests first, then the *text* group was allowed to also experience the Cyberherores interactive ebook and complete the usability evaluation at the end of the study (see Table 2). Results in Section 5.3 suggest no statistical significant differences in children's opinions of Cyberheroes between groups.

.

4.3. Data Analysis

Interviews. The transcriptions of the audio recorded responses were organized in Excel according to the interview questions. Two researchers coded all responses independently based on a pre-agreed answer key. A score of 3 is allocated for an "excellent response", 2 for a "marginal response", and 1 for a "poor response". The interviews were scored out of 12 points for *privacy knowledge*, and 18 points for *privacy behaviour* on each test. The two scores were then added to obtain children's total privacy proficiency score for a maximum of 30 points. A Cohen's Kappa (k) test showed very strong agreement between the two researchers' analysis of the Pre-Test ($k = 0.972$, 95% CI: 0.945 to 0.999, $p < 0.001$), Post-Test ($k = 0.977$, 95% CI: 0.952 to 1.000, $p < 0.001$), and 1-Week-Test ($k = 0.947$, 95% CI: 0.908 to 0.986, $p < 0.001$). In cases of disagreement, mean scores between the two researchers were used in the analysis.

Co-Reading Interaction and Discussion. Children and parents' co-reading sessions were audio recorded and timestamped. To measure child-parent discussions during reading, we transcribed portions of the audio when parents or children deviated from reading the main text, and logged the start and end of the audio segments with timestamps. Total discussion duration was obtained from summing the length of segments for each pair.

	Pre-Test		Post-Test		1-Week-Test				
Cond.	M	SD	M	SD	M	SD	$F(2, 20)$	p (<)	η^2
Ebook	19.409	4.779	24.000	3.324	24.500	2.828	20.515	**.001**	.672
Text	17.864	4.910	22.909	3.419	20.682	4.291	12.942	**.001**	.564

Table 3: One-Way Repeated Measures ANOVA showing statically significant effect in both conditions for children's privacy proficiency over three time points. M = Mean, SD = Standard Deviation, F = F-ratio, p = Significance Level, η^2 = Partial Eta Squared.

5. Results

5.1. Comparing the Effects of Cyberheroes and the Control on Children's Privacy Proficiency

Figure 2 and Table 3 show children's mean privacy proficiency scores per group, measured at pre-reading, post-reading, and 1-week post-reading. We first conducted one-way repeated measures ANOVA to determine whether there was an effect of time on children's privacy proficiency test scores. The data in both groups was normally distributed and the assumption of sphericity was met.

The results in Table 3 showed that children in both groups had a significant increase in privacy proficiency over time, particularly pre- and post-reading, and pre- and 1-week post-reading, as indicated by post hoc test results with Bonferroni adjustment in Table 4. As it is expected, there was no statistically significant effect between post-reading and 1-week post-reading scores in either groups. However, the *text* group showed a decrease in their privacy proficiency scores in the 1-Week-Test (illustrated in Figure 2), suggesting that the ebook group was more successful at maintaining 1-week learning effects.

To investigate this observation further, we followed up with one-way Analysis of Covariance (ANCOVA) tests to interpret whether there are differences in children's privacy proficiency scores between the two conditions after controlling for pre-reading privacy proficiency scores[4].

[4]We used children's Pre-Test privacy proficiency scores as a covariate due to the assumption that their post-reading performance is somewhat dependent on their pre-reading knowledge.

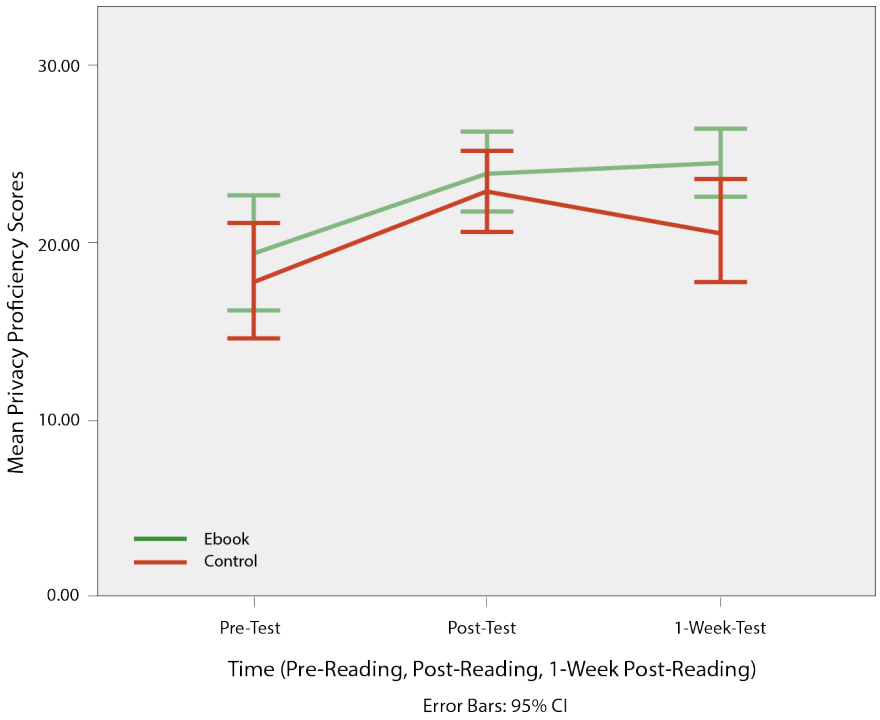


Figure 2: Comparison of the *ebook* & and *text* groups' privacy proficiency scores over time.

	Ebook			Text		
Time	MD	95% CI	p	MD	95% CI	p
Pre/Post	4.591	[2.278, 6.903]	**.001**	5.045	[1.983, 8.108]	**.002**
Pre/1-week	5.091	[2.069, 8.112]	**.002**	2.818	[.012 to 5.624]	**.049**
Post/1-week	.500	[1.620, 2.620]	1.000	2.227	[.449, 4.904]	.114

Table 4: One-Way Repeated Measures ANOVA with Post hoc tests showing statistically significant increase in both conditions in privacy proficiency in the Pre/Post-Test and Pre/1-Week-Test, but not in the Post/1-Week-Test. MD = Mean Difference, CI = Confidence Interval, p = Significance Level.

		Unadjusted		Adjusted	
	N	M	SD	M	SE
Ebook	11	24.500	2.828	24.083	.786
Text	11	20.682	4.291	21.099	.786

Table 5: Adjusted and unadjusted means and variability for the 1-Week-Test privacy proficiency scores with Pre-Test privacy proficiency scores as a covariate. N = Number of Subjects, M = Mean, SD = Standard Deviation, SE = Standard Error.

The assumptions for the ANCOVA were met, including a linear relationship between the data, homogeneity of regression slopes, normal distribution, homoscedasticity, homogeneity of variances, and an absence of outliners. With adjustments for the Pre-Test privacy proficiency scores, the results revealed no statistically significant difference in the Post-Test scores between the conditions, $F(1, 19) = .077$, $p = .784$, partial $\eta^2 = .004$. In other words, children in both conditions increased their privacy proficiency after reading. One week later however, there was indeed a statistically significant difference in the 1-Week-Test privacy proficiency scores between the conditions, $F(1, 19) = 7.102$, $p = .015$, partial $\eta^2 = .272$. A comparison of the adjusted and unadjusted means of the 1-Week-Test privacy proficiency scores by the covariate (i.e., Pre-Test privacy proficiency scores) is summarized in Table 5. This further supports the result that the Cyberheroes interactive ebook had superior 1-week learning effects on children's privacy proficiency than the control.

5.2. Co-reading Interactions

Parent-child co-reading time, duration of privacy discussions, and reading format are summarized in Table 6. Both groups showed various co-reading preferences. The narrative stimulated parents in both groups to ask children questions such as, "what do you think is the difference between a cyberhero and a cybervillian?" (P3-ebook), or "if cyberheroes are the good people who are the cybervillians?" (P6-text). The children would give responses such as "the heroes try to save all the privacy" (C3-ebook), and the cybervillians are "the

	Total Reading Time	Time Discussing Privacy	Co-Reading Format			
			P Read to C Aloud	P & C Read Aloud	C Read Aloud	C Read Silently
Ebook	8:52	2:02	7	3	0	1
Text	5:42	0:59	6	2	3	0

Table 6: Parent-child total co-reading time, time spent on privacy discussions, and co-reading formats. 'P' = Parent, 'C' = Child. Time is shown in minutes.

bad people" (C6-text). However, the interactive ebook motivated more meaningful discussions through interactions with the interface. The interactive ebook prompted 2:02 minutes of child-parent discussions compared to 59 seconds for the control. Children asked parents questions while referring to onscreen text, images, and interactions, while the *text* group solely relied on the story. Children used all interactive features, and two children read Cyberheroes more than once. Children spent the longest time on online chatting (Figure 1B), personal information, and cyberpowers (Figure 1D), and interacted with the content multiple times to activate sound effects and animations, suggesting these screens were the most engaging for children. To demonstrate the types of child-parent interactions that took place, we give P8-ebook and C8-ebook's conversation while using the online chatting screen as an example:

- *Child taps on a character on screen who appeared to be 8-year-old Alex, but the imaged changed to 42-year-old Mr. R.*
  - *Parent:* So he's not Alex, he's Mr. R, so he is lying; he is using a disguise. [The parent points to another character] So is that aunt Peggy?
  - *Child:* [Taps the character and the image changed to aunt Peggy] Yup!
  - *Parent:* [The parent points to another character] "Is that kitty?"
  - *Child:* [Taps the character and the image changed to 36-year-old Erin] Uh, it's not.
  - *Parent:* "That's Erin, she's 36 years old and she's pretending to be a cat."
  - *Child:* "So those two are liars and those two are true friends."

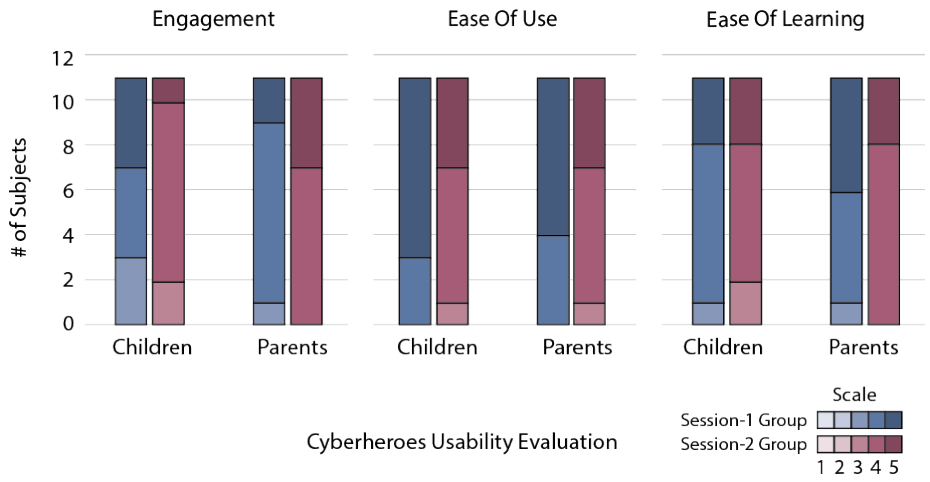


Figure 3: Summary of children and parents' usability evaluations of the Cyberheroes interactive ebook on engagement, ease of use, and ease of learning on a 5-point Likert-scale, where 5 is most positive.

Many parents in the ebook group supplemented the narrative and interaction with real life examples, such as incidents of Cyberbullying: P6-A said to C6-A "remember that [your sister] went through [cyberbullying] with some people at school? They were rude online to each other."

5.3. Usability of Cyberheroes

Parents' Pre-Evaluation (rank 1 = most important) showed that they thought fun ($M = 2.8$), age-appropriateness ($M = 2.8$), educational value ($M = 2.7$), and effectiveness ($M = 3.0$) are near equally important features for children's educational ebooks. Ease of use ($M = 3.8$) was ranked the least important because parents felt adults could assist children.

We did not find gender effects or between-group effects in the usability evaluations of Cyberheroes. Mann-Whitney U tests showed no statistically significant differences between gender (Engagement: $U = 39, Z = -1.285, p = .199$; Ease of Use: $U = 54, Z = -.155, p = .876$; Ease of Learning: $U = 29.5, Z = -2.058, p = .070$), or between conditions (Engagement: $U = 52, Z = -.618, p = .537$; Ease

of Use: $U = 37, Z = -1.758, p = .079$; Ease of Learning: $U = 56.5, Z = -.299, p = .765$). However, to avoid possible bias caused by the *text* group's reading of the text-only format prior to reading the interactive ebook, we present the usability results between the two groups independently. In the following section, we refer children and parents who read the ebook in the first session as the "session-1 group", and those who read the ebook in the second session as the "session-2 group". Usability evaluations of Cyberheroes from all 22 children and 22 parents were consistently positive. Figure 3 shows a comparison of their evaluations on "engagement", "ease of use", and "ease of learning".

Cyberheroes is engaging for children. The Smileyometer and the Again-Again Table from the Fun Toolkit [35] were used to measure engagement. Reed and MacFarlane [35] found high correlations between them for measurements of engagement (i.e., fun), suggesting that they are assessing the same construct.

Results from the two instruments showed that children found Cyberheroes fairly engaging. Figure 3 shows their Smileyometer evaluations for engagement. Furthermore, the Again-Again Table evaluations showed a mean score of 2.27/3 for the session-1 group ($n = 3$ for "yes", $n = 8$ for "maybe", $n = 0$ for "no") and 2.45 for the the session-2 group ($n = 6$ for "yes", $n = 4$ for "maybe", $n = 1$ for "no"). Other aspects of the evaluation showed that children found the characters likeable (session-1 and session-2 groups: $M = 3.82$), and were willing to recommended Cyberheroes to others (session-1 and session-2 groups: $M = 3.82$). Open-ended feedback suggested that children highly enjoyed the interactive features and the superhero theme. They particularly liked "pressing the stars"[5] to show cause and effect relationships. For example, C6-ebook said, I liked "pressing the stars because we could figure out if they are good guys or bad guys." Children liked that at the end of the story "everyone became cyberheroes" (C7-text).

Parent also found Cyberheroes engaging. Most are very willing to read it

[5]Interactive features in Cyberheroes are marked with an animated star.

again with their child (session-1 group: $M = 4.73$, session-2 group: $M = 4.64$). They thought the interactive ebook was fun; the superhero angle facilitated "direct connection of identity with the topics" (P2-ebook); the characters were "gender inclusive" (P9-ebook), and "true to life with nine and seven-year-old siblings" (P5-text).

Cyberheroes is easy to use for children. Both children and parents found Cyberheroes very easy to use. We did not observe any children having difficulties interacting with the interface. Only one child (C6-text) would have preferred to have narration audio in addition to the onscreen text. Parents suggested avoiding using big words like "empathy" and "gossip" in the narrative, but children were able to overcome any misunderstandings by asking parents for help. Overall, Cyberheroes "was very easy for children to understand" (P9-text). Parents thought the interactive ebook "was simple to read and talk together" (P5-text), "easy to create discussion about privacy", and "very informative and right to the point" (P3-ebook).

Cyberheroes made learning easy for children. Children felt they learned well from Cyberheroes. They enjoyed "learning what things that Bobby and Ally should or shouldn't do" (C3-ebook). C1-ebook said, "I liked that the book teaches about the Internet and what you should or should not do, like you shouldn't trust anyone, and shouldn't give out personal information to people." The characters showed "how they put everything on the Internet because they didn't practice their cyberpowers" (C7-text). Children felt that the interactions in the ebook "made it interesting," as if " the story happened for real" (C8-text).

Parents also thought Cyberheroes was an effective learning tool for children. The ebook was a "good introduction to the concepts, basic enough to prompt the child to ask for more information and details about what's going on" (P6-ebook). It "introduced danger without scaring them" (P10-ebook), and achieved explaining privacy at an elementary level that is very attractive to children, which "increased their interest to read to the end of the story" (P8-text).

Other aspects of parents' evaluations showed they interacted well together with their child (session-1 group: $M = 4.45$, session-2 group: $M = 4.27$). They said Cyberheroes was very educational (session-1 group: $M = 4.36$, session-2 group: $M = 4.64$) and age-appropriate for children (session-1 group: $M = 4.27$, session-2 group: $M = 4.36$). The tool was effective at facilitating child-parent privacy conversations (session-1 group: $M = 4.09$, session-2 group: $M = 4.18$). Parents were willing to use the educational tool with their children (session-1 group: $M = 4.91$, session-2 group: $M = 4.64$). As one parent puts it, "some learning came from the book itself, and some came from the conversations we had" (P10-ebook).

6. Discussion

Our study provides some insights into how to introduce children to online privacy concepts at an early age, and how an interactive tool could assist parents in starting a conversation about these issues with children.

6.1. Knowledge Acquisition, Retention, and Transfer

Schmidt and Bjork [36] describe knowledge acquisition, retention, and transfer as the three phases of learning. *Knowledge acquisition* determines how well the learner can process and extract knowledge. In our study, children in both our conditions acquired knowledge and significantly improved their privacy knowledge post-reading.

Knowledge retention measures learners' ability to retain and recall information after some time. Children who viewed Cyberheroes scored higher on privacy proficiency tests after one week than those who read the text-only narrative, demonstrating that the ebook assisted in knowledge retention. Cyberheroes included text, images, sounds, and user interaction. As discussed in Section 2, past work cautioned that some multimedia features could act as distractors [15] and hinder comprehension [16]. However, our experience were mainly positive.

Our results align with Paivio's dual coding theory [37], which states that the combination of related text and images enhance comprehension and increase

long-term memory. Education literature also supports the theory that depicting the content of accompanying text facilitates the construction of a lasting mental model [38]. In the present study, we observed that user interaction contributed to mental model building. For example, on "digital trail" screen in Cyberheroes (see Figure 1C), children performed an interaction where he/she attempted to "erase" the digital trail with a giant eraser, which led to parent-child conversations such as, "you can try to erase it but what happens? If we erase it is it still there?" (P3-ebook); "yes" (C3-ebook). Our study lends further evidence of the benefits of visuals and interaction to help build mental models.

Knowledge transfer is the learner's ability to apply acquired knowledge to a closely related context (near transfer) and to different situations (far transfer). Our assessment of children's responses to different scenarios suggested that Cyberheroes better supported both near and far knowledge transfer than the control condition. For example, C9-ebook described personal information as "stuff that you don't want to tell other people, like where you live, what your password is..." When asked about what she would do if her best friend asked to borrow her password, she was able to explain why passwords should be kept private, therefore demonstrating near transfer of knowledge: "I wouldn't give her my password, because she could tell other people my personal stuff." Children also demonstrated far transfer of knowledge in their response to alternate scenarios in the 1-Week-Test. For example, C9-ebook was able to recognize cyberbullying in different contexts and realize that her response would still be applicable; she gave the same response ("I wouldn't send a message back, and tell mama and papa.") when cyberbullying was aimed towards herself (Post-Test scenario) or towards another kid (1-Week-Test scenario).

Knowledge transfer is particularly important in the domain of security and privacy because of the rapid evolution of threats. Furthermore, many risks include aspects of social engineering where attacks actively try to deceive potential victims. Children need to develop critical thinking skills where they can reason about new situations and recognize new risks that may not look exactly like those they have learned about previously.

6.2. Effect of Interactivity

As mentioned above, we found an overall positive influence from the interactive components included in Cyberheroes. Interactivity increased children's engagement with the ebook itself, with participants spending more time actually reading and interacting with the ebook than the text-narrative. It also increased engagement between the child and their parent; we observed them spending more time having privacy-related conversations and expanding on the content of the story. And perhaps most importantly, these interactions led to increased knowledge retention and knowledge transfer.

6.3. Leveraging Previous Knowledge

Security and privacy are complex and potentially abstract concepts. Prior work [24, 39, 40, 41, 25] suggests that adults have poor mental models of security. Not surprisingly, our work showed that children also exhibit poor mental models that are even less sophisticated than those of adults. We found that children rely on their experiences with physical privacy and safety to navigate online spaces [26]. We believe that a reasonable approach is to leverage children's existing understanding of parallel concepts in the physical world to communicate online privacy risks. We used this approach in Cyberheroes and found children could easily relate to concepts of identity, physical privacy, and safety. For example, in Cyberheroes, passwords are used to protect a vault, a physical map is used to trace Bobby's location, an eraser is used to delete digital information. By grounding explanations in concepts that are already understood, we can help children use their experience to reason about new online situations in ways that helpm rather than hinder, formation of adequate mental models.

6.4. Respecting Family Dynamics and Sensibilities

Parents want to educate children about online risks, but they also want to shelter them from online negativity [26]. They have varying opinions about the appropriate age for accessing various types of online tools and services like social media, and were thus cautious about children's early exposure to these subjects.

Young children's primary online activities are playing games, watching video clips, instant messaging, and doing school work [42, 1, 2]. Many children do not manage their own online accounts, passwords, and online purchases (e.g., apps) [26]. Parents are thus involved in children's daily interaction with technology and share the responsibility for managing children's privacy and security [43].

Furthermore, today's children are digital natives. Many aspects of their lives either directly involve online interaction or have been documented online by others, such as their caregivers. The concept of online privacy is evolving and families have different tolerance for online sharing and privacy-preserving behaviours. Whereas other types of safety education, such as how to cross the street or how to handle sharp objects, are fairly static in their instruction; the topic of online privacy can be approached very differently by different families. Privacy education material designed for young children should respect the preferences of families and their sensibilities toward media and technology.

We also found that families have different dynamics and interaction styles, such as how they engaged in co-reading. A 2010 study showed that reading ebooks with adult instruction effectively improved children's literacy compared to no adult instruction [7]. Cyberheroes introduced children to essential online privacy concepts at an elementary level and inspired them to ask parents for more information about what they read. This empowers parents to disclose more information about specific topics at a level that they deem relevant and appropriate for their child. Generally though, privacy education designed for young children should gently introduce privacy and safety concepts without scaring them and should avoid topics that are irrelevant for their age.

6.5. Limitations and Future Work

Some limitations of our work include that the sample size is small and not geographically diverse, and that the long-term effects of learning are limited to one week. We also could not control for variability of dynamics within our participating families. Future work could study the long-term effects of the

education tool on children's privacy proficiency and how parents and children would interact with it at home. It would also be interesting to study how such privacy education tool could be adapted into the classroom setting in early elementary years as a instructional tool for teachers.

7. Conclusion

Computer security and privacy concepts are complex and difficult to learn even for adults. We address the challenge of transforming essential privacy information into an engaging format that resonated with young children. Cyberheroes significantly improved children's privacy proficiency and successfully supported parents in explaining privacy concepts to children.

The research findings provide evidence that images and interactive elements in ebooks support children's knowledge acquisition, retention, and transfer. Furthermore, interactive ebooks are useful in fostering child-parent discussions about the content that could lead to extended learning. We suggest that online privacy education efforts need take into consideration that parents are sensitive towards children's exposure to 'frightening' topics or educational material that is inappropriate for their age. We showed that one way to communicate to children about a potentially serious and abstract topic such as online privacy is to leverage previously understood concepts to construct adequate mental models that children could use to reason about new online situations.

8. Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security.

References

[1] V. Rideout, Zero to eight: Children's media use in America: A Common Sense Media research study, https://www.commonsensemedia.org/research/ (2013).

[2] V. Steeves, Young Canadians in a wired world, phase III: Life online, http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf (2014).

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

[4] O. Korat, Reading electronic books as a support for vocabulary, story comprehension and word reading in kindergarten and first grade, Computers & Education 55 (1) (2010) 24–31.

[5] T. Jones, C. Brown, Reading engagement: A comparison between e-books and traditional print books in an elementary classroom., International Journal of Instruction 4 (2) (2011) 5–22.

[6] Y.-M. Huang, T.-H. Liang, Y.-N. Su, N.-S. Chen, Empowering personalized learning with an interactive e-book learning system for elementary school students, Educational Technology Research and Development 60 (4) (2012) 703–722.

[7] O. Segal-Drori, O. Korat, A. Shamir, P. S. Klein, Reading electronic and printed books with and without adult instruction: Effects on emergent reading, Reading and Writing 23 (8) (2010) 913–930.

[8] J. Piaget, Judgement and reasoning in the child, Routledge, 2002.

[9] M. L. Guha, A. Druin, G. Chipman, J. A. Fails, S. Simms, A. Farber, Mixing ideas: A new technique for working with young children as design partners, in: Interaction Design and Children, ACM, 2004, pp. 35–42.

[10] H. R. Schugar, C. A. Smith, J. T. Schugar, Teaching with interactive picture e-books in grades K–6, The Reading Teacher 66 (8) (2013) 615–624.

[11] L. Colombo, M. Landoni, A diary study of children's user experience with ebooks using flow theory as framework, in: Interaction Design and Children, ACM, 2014, pp. 135–144.

[12] C. J. Pearman, Independent reading of CD-ROM storybooks: Measuring comprehension with oral retellings, The Reading Teacher 61 (8) (2008) 594–602.

[13] S. Grimshaw, N. Dungworth, C. McKnight, A. Morris, Electronic books: Childrens reading and comprehension, British Journal of Educational Technology 38 (4) (2007) 583–599.

[14] M. J. Verhallen, A. G. Bus, M. T. de Jong, The promise of multimedia stories for kindergarten children at risk., Journal of Educational Psychology 98 (2) (2006) 410.

[15] M. T. de Jong, A. G. Bus, How well suited are electronic books to supporting literacy?, Journal of Early Childhood Literacy 3 (2) (2003) 147–164.

[16] R. Garner, M. G. Gillingham, C. S. White, Effects of 'seductive details' on macroprocessing and microprocessing in adults and children, Cognition and instruction 6 (1) (1989) 41–57.

[17] N. Dalla Longa, O. Mich, Do animations in enhanced ebooks for children favour the reading comprehension process?: A pilot study, in: Proceedings of the 12th International Conference on Interaction Design and Children, ACM, 2013, pp. 621–624.

[18] O. Korat, A. Shamir, Electronic books versus adult readers: Effects on children's emergent literacy as a function of social class, Journal of Computer Assisted Learning 23 (3) (2007) 248–259.

[19] A. Dünser, E. Hornecker, An observational study of children interacting with an augmented story book, in: Technologies for E-Learning and Digital Entertainment, Springer, 2007, pp. 305–315.

[20] K. Roskos, J. Brueck, S. Widman, Investigating analytic tools for e-book design in early literacy learning, Journal of Interactive Online Learning 8 (3) (2009) 218–240.

[21] A. Whitten, J. Tygar, Why Johnny can't encrypt: A usability evaluation of PGP 5.0, in: USENIX Security, 1999.

[22] C. Herley, So long, and no thanks for the externalities: the rational rejection of security advice by users, in: Proceedings of the 2009 workshop on New Security Paradigms Workshop (NSPW), ACM, 2009, pp. 133–144.

[23] K. Craik, W. James, The Nature of Explanation, Cambridge University Press, 1967.

[24] R. Wash, Folk models of home computer security, in: Symposium on Usable Privacy and Security (SOUPS), ACM, 2010.

[25] F. Asgharpour, D. Liu, L. Camp, Mental models of security risks, Financial Cryptography and Data Security (2007) 367–377.

[26] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, S. Chiasson, From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats, in: Interaction Design and Children, ACM, 2016, pp. 388–399.

[27] A. Druin, The role of children in the design of new technology, Behaviour and information technology 21 (1) (2002) 1–25.

[28] R. Clark, R. Mayer, E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning, John Wiley & Sons, 2011.

[29] D. A. Norman, The design of everyday things: Revised and expanded edition, Basic books, 2013.

[30] B. Shneiderman, Designing the user interface: strategies for effective human-computer interaction, Pearson Education India, 2010.

[31] J. Nielsen, Heuristic evaluation, Usability inspection methods 17 (1) (1994) 25–62.

[32] J. P. Hourcade, Interaction design and children, Foundations and Trends in Human-Computer Interaction 1 (4) (2008) 277–392.

[33] L. S. Vygotsky, Mind in society: The development of higher psychological processes, Harvard university press, 1980.

[34] J. Scott, Children as respondents: The challenge for quantitative methods, Research with children: Perspectives and practices (2000) 98–119.

[35] J. C. Read, S. MacFarlane, Using the fun toolkit and other survey methods to gather opinions in child computer interaction, in: Interaction Design and Children, ACM, 2006, pp. 81–88.

[36] R. A. Schmidt, R. A. Bjork, New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training, Psychological Science 3 (4) (1992) 207–217.

[37] J. M. Clark, A. Paivio, Dual coding theory and education, Educational Psychology Review 3 (3) (1991) 149–210.

[38] V. Gyselinck, H. Tardieu, The role of illustrations in text comprehension: What, when, for whom, and why?

[39] P. Dourish, R. E. Grinter, J. D. De La Flor, M. Joseph, Security in the wild: User strategies for managing security as an everyday, practical problem, Personal and Ubiquitous Computing 8 (6) (2004) 391–401.

[40] J. B. Gross, M. B. Rosson, Looking for trouble: Understanding end-user security management, in: Symposium on Computer-Human Interaction For the Management of Information Technology, ACM, 2007, p. 10.

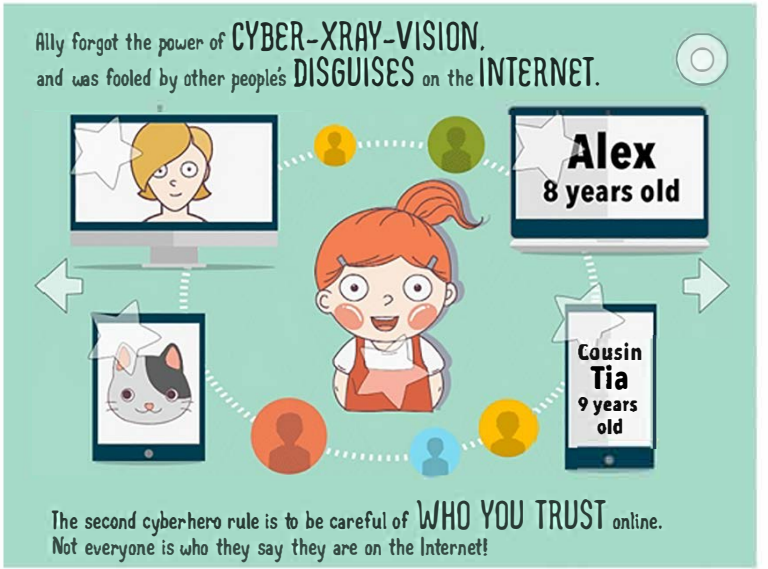
[41] R. E. Grinter, W. K. Edwards, M. W. Newman, N. Ducheneaut, The work to make a home network work, in: Computer Supported Cooperative Work, Springer, 2005, pp. 469–488.

[42] S. Livingstone, M. Bober, Uk children go online: Surveying the experiences of young people and their parents.

[43] T. Ammari, P. Kumar, C. Lampe, S. Schoenebeck, Managing children's online identities: How parents decide what to disclose about their children online, SIGCHI Conference on Human Factors in Computing Systems.


cyberheroes

A.


Ally forgot the power of CYBER-XRAY-VISION,
and was fooled by other people's DISGUISES on the INTERNET.
Alex
8 years old
Cousin
Tia
9 years
old
The second cyberhero rule is to be careful of WHO YOU TRUST online.
Not everyone is who they say they are on the Internet!

B.


Ally and Bobby didn't care. "We could just delete everything" they thought.
They tried to erase their digital trail, but the tracks wouldn't disappear.
They are on
the internet
FOREVER
& EVER!

C.


Then, they realized that all the children could have cyberpowers.
You only have to LEARN and PRACTICE them.
CYBER-DISGUISE
Never, ever provide your personal information to anyone
CYBER-X-RAY
Be careful of who you trust onl ne
CYBER-INVISIBILITY
Never reveal where you are, especially to strangers
CYBER-EMPATHY
Be kind to others
CYBER-PASSWORD
Always keep your passwords to yourself

D.