‘Lime’, ‘Open Lock’, and ‘Blocked’: Children’s Perception of Colors, Symbols, and Words in Cybersecurity Warnings

Rebecca Jeong
Carleton University
Ottawa, Canada
beckyjeong@gmail.com

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

ABSTRACT

Cybersecurity warnings are frequently ignored or misinterpreted by even experienced adults. While studies have been conducted to examine warning design for adults, there is little data to establish recommendations for children. We conducted user studies with 22 children (ages 10-12) and with 22 adults. We compare their risk perception of warning design parameters (signal colors, symbols, words) via card sorting and ranking activities followed by interviews. While our findings suggest similarities in how both groups interpret the design parameters (e.g., `red`, `skull`, and `fatal` convey danger), we also uncovered potential concerns with items currently used as security indicators (e.g., both groups had mixed interpretations of the `open lock` and `police officer` symbols). Individual risk perception, particularly for children, appears dependent on personal preferences and experience. Our findings suggest implications and future research directions for the design of cybersecurity warnings for children.

Author Keywords

Children, Risk Perception, Cybersecurity Warnings

CCS Concepts

•**Security and privacy** → **Human and societal aspects of security and privacy; Usability in security and privacy;**

INTRODUCTION

29% of users underwent a malware attack in 2017, and the US and Canada were among the top 10 countries where online resources contained malware [29]. Cybersecurity warnings are intended to help protect users from such threats [8]. However, warnings are often ignored or misinterpreted even by experienced adult users [1,8]. Even when risk is imminent, people do not read, understand, or heed to computer warnings [1, 8, 44].

Improving security warnings is imperative to properly alert users of threats, and to encourage them to take appropriate security measures [8]. The *human-in-the-loop* (HITL) security framework [10] suggests that warnings that communicate risk effectively can help mitigate threats. Warning *design parameters* (i.e., design components [2]) include signal colors, symbols, and words, among others. These cue users to the severity of the threat, and help them determine how much attention and credibility to allocate to the warnings. To be effective, the level of hazard intended by the designer must match the level of hazard perceived by the user [2].

While studies have been conducted with adults to examine warning design (e.g., [2, 12, 19–21, 31, 52]), there are few empirical studies to establish recommendations for children (e.g., [16, 37, 53]). It is unclear whether children interpret the design parameters in the same way as adults. Children are one of the fastest growing groups of online users, with those under 18 accounting for one in three internet users worldwide [47]. According to UNICEF’s Executive Director, *“digital policies, practices, and products should better reflect children’s needs, children’s perspectives, and children’s voices”* [45].

When we shift our focus from adults to children, privacy and security issues become more complicated [56]. Children may be particularly vulnerable due to their poor understanding of online threats [56, 57] and they may not understand the consequences of their actions. To help children make safer choices online, we must communicate in ways that are meaningful to them. As a starting point, this research explores children’s interpretation of various design parameters for cybersecurity warnings. We focus on signal colors, symbols, and words, used to signal potentially harmful situations [2]. We also explored adults’ perspective of cybersecurity warnings to serve as a baseline since these warnings are typically designed for adults [16, 37]. We explore the following research question:

RQ. *How do children and adults compare in their perceptions and understanding of signal colors, symbols, and words in the context of cybersecurity warnings?*

Our studies identify similarities and differences between children and adults’ perception of warning design parameters. First, we provide data on children’s perceived level of hazards for signal colors, symbols, and words. Second, we identify how the two groups compare in their perceptions of, previous experiences with, and expectations for cybersecurity warnings. Third, we identify concepts and associations that shape children and adults’ risk perceptions, and help them to determine what is dangerous or safe. Finally, we discuss implications for the design of cybersecurity warning messages for children.

CHI ’20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376611

BACKGROUND

Warnings

Warnings are a type of communication designed to prevent people from harm [4, 8, 50]. They can include information on the presence of hazards and instructions on how to avoid them [8, 19, 51]. Warnings can alert users of threats, remind users, or trigger change in user behaviour [8]. When systems cannot eliminate risk or completely protect users from harm, warnings are used as the next line of defense [1, 3, 8, 10, 44, 51].

Bravo-Lillo *et al*. [8] argue that cybersecurity warnings should protect users and their computers, and that humans' psychological process in heeding, understanding, and complying with such warnings is similar to that of physical warnings. Whether physical or digital, humans respond better to warnings that communicate risk clearly, explain consequences of noncompliance, and provide instructions on how to comply [8, 51]. Warning design should consider the type of communication that will be the most effective, the severity of the hazard, and how much user action is required to avoid the hazard [10].

Warning Design Parameters

Signal Colors

Signal colors are a common design parameter for physical and digital warnings [43]. Silic *et al*. [43] emphasized that color is a significant determinant of perceived risk and intentions to comply. Braun *et al*. [6] found that warning labels presented in color were perceived to be more hazardous and readable than those presented in black-and-white. Humans have the tendency to associate colors with everyday events, social norms, and attributes. For example, in western cultures, the colors *pink* and *blue* are generally used to differentiate between girls and boys, and *black* is worn for mourning [19, 25]. Literature on affective colors show that younger children tend to love and are attracted to things that are bright and bold [18]. Boyatzis and Varghese [5] found that children 5 to 6 years old associated bright and light colors (e.g., *red, yellow, orange, blue, pink*) with positive emotions (e.g., happiness, excitement, comfort), and dark colors (e.g., *black, grey, brown*) with negative emotions (e.g., sadness, anger). In a study examining college students' color-emotion associations, Kaya and Epps [25] found that lighter and cooler hues (e.g., *green, blue, white*) were generally seen to be positive while darker shades (e.g., *black, grey*) elicited negative emotions. The perception of some colors differed for adults compared to children. For example, the college students believed that *red* had both positive (e.g., love, romance) and negative connotations (e.g., evil, blood) [25].

Red has negative connotations in cyberspace [43]. *Red* is often used to denote high risk and to grab human attention [19, 22, 31, 43]. Using differential and free-association techniques, Griffith and Leonard [19] found *red* most strongly associated with high levels of perceived hazard among adults.

General standards for physical warnings suggest that different colors imply varying levels of risk (e.g., *red-danger*, *orange-warning*, *yellow-caution*, *blue-notice*) [19, 31]. Leonard [31] examined the perception of risk for color words in the context of warning signs using a seven-point Likert scale. *Red*, *orange*, *black*, and *yellow* were rated most risky by his adult participants. Colors *white*, *blue*, and *green* were considered the least serious. Similarly, Holtzschue [22] suggests that some colors are important in communicating ideas. The US Occupational Safety and Health Administration (OSHA) colors include *yellow* for *caution*, *orange* for *dangerous machinery or equipment*, *red* for *danger* and *stop*, and *green* for *safety*.

The relationship between colors, other design parameters, and 'contextual associations' has also been explored. Griffith and Leonard [19] found that *red* was highly associated with the word *stop* and the *traffic stop sign*. They also associated *yellow* and *red* with *traffic lights*, *caution*, and *warning*. *Black* was associated with signal words such as *fatal*, *deadly*, and *poison*, and symbols such as *skull*, a sign of death [19].

Signal Symbols

Symbols and patterns are important for attracting users' attention [12]. By increasing salience, warnings with symbols are more likely to gain attention compared to those without [2, 52]. Wogalter *et al*. [52] explain that symbols allow users to easily comprehend warnings visually, especially for young children, and for users who speak a different language or are illiterate. When designed correctly, symbols in warnings are able to reach and convey risk to the general population more effectively. The researchers also recommend testing symbols and text prior to implementation to ensure their effectiveness [52].

Amer and Maris [2] examined the *arousal strengths* of signal symbols in IT exception messages (i.e., the severity or level of hazard communicated by the items). In adults, *X* had the highest perceived arousal strength, followed by *!*, *?*, and *i* [2]. Exploring the impact of shapes on the perception of warning signs, Ma *et al*. [32] found that adults have a stronger negative interpretation of the *upright triangle* than of the *circle*.

Signal Words

Words such as *danger*, *warning*, *caution*, and *notice* are considered standard for physical warnings, and are intended to elicit different levels of risk perception in users [19]. In Griffith and Leonard's study [19] on physical warnings, *danger* had the highest arousal strength. Leonard [31] found that the words *fatal*, *deadly*, *danger*, and *warning* were considered very severe, and *notice*, *attention*, and *caution* were less serious in adults.

Hellier *et al*. [20, 21] highlighted the importance of mapping signal words to the level of risk implied by the hazard. They suggest that words that do not imply an explicit risk should be avoided in severe warning messages. For instance, *careful* may be used in hazardous situations while *notice* should not [20]. Amer and Maris [2] found that on exception messages, adults found *critical* to have the highest perceived severity of hazard, followed by *urgent*, *warning*, *error*, and *notice*.

Warning Design and Guidelines for Adults

Current research on warning design and guidelines have mostly focused on adults. These studies have explored *inhibitive attractors* (i.e., to prevent users from proceeding until they interact with the warning or after a certain time has passed) and *non-inhibitive attractors* (i.e., eye-catching stylistic change of text font and background) [7, 9], and *polymorphic*

warnings (i.e., visual variations such as messages that jiggle, or change in size, color, symbols, or words) [3]. Wogalter *et al*. [52] presented an overview of general warning design and evaluation guidelines, and Bauer *et al*. [4] proposed an initial set of computer system warning design guidelines. While these studies provide helpful direction for designing warnings, little is known if the suggestions are also effective on children.

Warning Design and Guidelines for Children

Micheti *et al*. [38] identified guidelines for privacy policies that children and teenagers can easily comprehend. Several of their guidelines may be relevant for warnings as well, such as how to design textual elements for comprehension, how to structure the text, and the overall design. Fruth *et al*. [16] and Menzel *et al*. [37] proposed and evaluated smartphone security warnings for children, which included a combination of visual, acoustic, and haptic design elements. Zaikina-Montgomery and Silver [53] explored the interaction between icon, color, word, and warning message in children. These studies provide implications for designing warnings for children (i.e., children showing adequate reaction to the security threat, children's understandability and likelihood of avoidance for design parameters); however, they do not give us insights into why children have these responses and perceptions.

Research Gap

Children are online independently by age 10 [34]. Many use social networking, watch videos, and play games despite Terms of Use that restrict use to those 13 and over [36]. Children aged 11-12 communicate online and may be vulnerable, but believe that they are competent to protect themselves [33,35]. However, privacy and security studies on youth mostly focus on teenagers [27]. We believe that it is important to understand preteens because they are developmentally able to start recognizing warning messages, consider the possible consequences of their actions, and make logical decisions if information is presented in an age-appropriate manner. Security practitioners must understand their target users and the severity of hazard perceived by those users [1]. Currently, there is a lack of research exploring children and their perception of warning messages. To address this, we first explore how children and adults perceive the severity of hazard associated with signal colors, symbols, and words. Our empirical findings help establish children's perceptions of security warnings compared to adults, and help identify warning message design features that may communicate more effectively to children.

METHODOLOGY

Hazard Matching

Our research methodology was inspired by the works of Amer and Maris [2], Bravo-Lillo *et al*. [8], Hellier *et al*. [21], and Wogalter *et al*. [52]. *Hazard matching* occurs when the intended severity of hazard communicated by the warning matches the user's perceived severity [2, 21]. To achieve this, a systematic relationship between warning design parameters and users' perceived levels of hazard should be established [21]. The first step is to scale the perceived arousal strength of each design parameter (quantifiers of risk) by asking users to rate their severity [2, 20, 21, 52].

Study 1: Children				**Study 2: Adults**			
ID	*Age*	*Grade*	*Gender**	*ID*	*Age*	*Education*	*Gender**
C01	11	6	Male	**A01**	24	Bachelor's	Female
C02	11	6	Female	**A02**	26	No diploma	Male
C03	10	5	Female	**A03**	31	Doctorate	Male
C04	12	7	Male	**A04**	29	Bachelor's	Female
C05	10	5	Female	**A05**	51	Bachelor's	Female
C06	11	6	Male	**A06**	28	Doctorate	Male
C07	11	6	Male	**A07**	28	Doctorate	Male
C08	11	6	Male	**A08**	28	Master's	Male
C09	11	6	Female	**A09**	23	Master's	Female
C10	11	6	Female	**A10**	26	Master's	Female
C11	10	5	Male	**A11**	26	Master's	Female
C12	12	7	Male	**A12**	19	Bachelor's	Male
C13	11	6	Male	**A13**	31	Bachelor's	Male
C14	10	5	Male	**A14**	48	Master's	Male
C15	11	6	Male	**A15**	28	Doctorate	Female
C16	11	6	Male	**A16**	22	Bachelor's	Female
C17	11	6	Male	**A17**	25	Master's	Female
C18	11	6	Male	**A18**	22	Master's	Female
C19	12	7	Male	**A19**	19	Bachelor's	Female
C20	12	6	Female	**A20**	26	Bachelor's	Male
C21	10	5	Female	**A21**	23	Master's	Female
C22	11	5	Male	**A22**	18	Bachelor's	Male

**Gender = self-identified gender*

Table 1. Child and adult participant demographics.

We used sorting and ranking methods to scale the perceived arousal strength of items within each parameter. Since this method may be susceptible to response bias [21], we followed the activity with an interview to clarify the dimensions that were important to each participant, as suggested by Wogalter *et al*. [52]. Sorting and ranking were chosen because they seemed to be simpler for children, compared to techniques such as Likert rating and free modulus magnitude estimation [21].

Participants and Recruitment

Our study was cleared by our Institutional Review Board and was advertised as "Exploring the characteristics of cybersecurity warning messages". Participants were recruited through social media, posters, and snowballing. Sessions took place in a quiet space with a large table for card sorting, such as a lab on campus or public library meeting room that was familiar and comfortable for participants, where adequate privacy and confidentiality were provided. All adults and 16 children came to campus; 6 children chose the library. We obtained written consent from the parent/legal guardians and from adult participants, and verbal informed assent from child participants. Participants received $20 and the cost of parking if applicable.

We conducted two studies; the first with 22 child participants (ages 10-12; 15 male, 7 female) and the second with 22 adult participants (ages 18-51; 10 male, 12 female) (Table 1). Children were online for an average of 2.5 hours per day (*SD*=1.79, missing 5 data points), 5 days per week (*SD*=2.05). The most popular devices used by children to go online were iPads

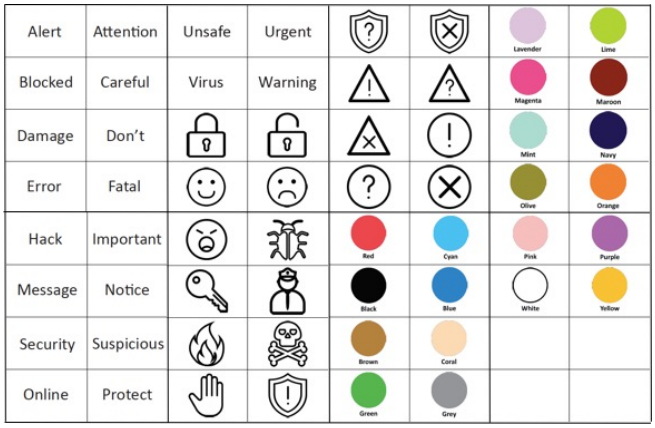

Figure 1. Cards used for card sorting and ranking activities.

(n=21) and laptop computers (n=21), desktops (n=15), iPhones (n=14), and Android phones (n=14). Adults had a wide range of educational backgrounds; all except one were currently enrolled in or had post-secondary education. Adults were online for an average of 8 hours and 15 minutes (SD=5.15) daily. The most popular devices used by adults were desktops (n=22) and laptop computers (n=22), iPhones (n=17), Android phones (n=17), iPads (n=17), and gaming consoles (n=15). All participants used more than one device to go online.

Materials

For the card sorting and ranking activities, we used 60 laminated standard size business cards that each had a different signal color, symbol, or word (Figure 1). The cards were created on Adobe Illustrator. To determine the specific signal items to include, we began with a literature review and web searches of existing cybersecurity warnings. We collected 80 examples of warnings from peer-reviewed articles, books, and conference proceedings, and search results from Google. The search results on warning messages included, but were not limited to, those on Mac, Windows, different web browsers (e.g., Chrome, Safari, Internet Explorer, Firefox), social networking services (e.g., Facebook, LinkedIn, Twitter, Instagram), and sample fake warning messages. From these examples, we extracted the most commonly repeated signal words, colors, and symbols, including some used outside of the cybersecurity context. For example, we extracted emotive symbols (e.g., `happy face, sad face, angry face`) that are similar to emojis used in electronic messages and web pages, and `fire` and `skull` symbols even though they were generally found on consumer products rather than cyberwarnings.

From our findings and the literature [19–21, 31], we gathered 36 common signal words. We ran a pilot study using a survey hosted on Qualtrics [41] and asked 6 security and design researchers to openly categorize the words with similar meanings into 20 self-selected, user-defined groups, and to rank them from most to least relevant for security in each group. We tabulated the results and selected the 20 highest ranked words. These 20 words were later printed on individual cards.

There were limited colors typically used in warning messages. For consistency, 20 colors were chosen from a palette of colors that were considered individually distinctive, including those commonly found on warning messages [19, 31]. Each color was printed on a card as a large colored circle with its name below it so that the participants could easily name them.

The 20 signal symbols chosen were simple, printed in black and white, and commonly found in general warning messages [2, 14, 15, 19, 39]. These were also printed on individual cards.

We printed large labels identifying the categories in which participants would sort the cards. The three categories identified the severity of hazard conveyed by the item on the card: 'Most Safe', 'Middle', and 'Most Dangerous'.

Protocol

Each session took approximately 1 hour, was audio-recorded, and transcribed by the research team. We conducted a short pre-test interview. For child participants, we asked for age, school grade, and self-identified gender. For adult participants, we asked for age, highest level of education completed or currently enrolled, and self-identified gender. We asked both groups about time spent online and electronic devices used.

We did not specify a context for the warnings. Before the card sorting, participants were asked: *"Imagine that you are online and you see a cybersecurity warning with this color/symbol/word on it. How dangerous/safe do you think this is?"* The cards were divided into three decks corresponding to the 3 conditions (colors, symbols, words). A Latin Square design was used to order the 3 conditions to mitigate order bias. Cards within each deck were randomly shuffled and presented to the participants one at a time. Participants sorted each deck on the table into 3 categories ('Most Safe', 'Middle', 'Most Dangerous'), then they ranked the cards within each category according to their perceived level of danger. Participants were encouraged to think-aloud and explain the rationale for their card placement. They could re-sort and re-categorize the cards as desired. If their explanations were unclear or ambiguous, we probed with open-ended questions about individual items such as, *"Could you explain why you placed that card in this category?"* The researcher took photos of the final card arrangements and transcribed those into a spreadsheet.

Participants verbally completed a post-test semi-structured interview regarding the perceived difficulty of categorizing the signal colors, symbols, and words, and their previous experience with cybersecurity warnings. We asked participants to tell a story about a time they came across a warning message, and asked them to explain what they would expect to see on a dangerous warning. Participants were encouraged to expand on their answers to give more context.

Data Analysis

We draw from more than 44 hours of transcribed audio-recordings with 22 child and 22 adult participants. We gathered the questionnaire responses, transcripts, and the results of the card sorting and ranking activities from the notes, comments, and photos taken by the primary researcher.

Quantitative Analysis Approaches

Following the categorization, participants were asked to rank the cards placed in each category to give them a smaller set

Theme	Definition
Level of danger	An assessment by the participant of the perceived safety or danger of a *signal item** (e.g., *safe* or *dangerous*).
Association with same parameters	The participant specifically mentions associations (similarities or differences) with other items in the same deck of cards (e.g., `red` and `maroon`).
Association with other parameters	The participant specifically mentions associations (similarities or differences) with items in a different deck (e.g., `black` and `skull`).
Contextual associations	The participant specifically mentions associations relating to other contexts (e.g., technology, food).
Subjective perception	The participant's subjective attitudes and perceptions in relation to a *signal item** (e.g., attention grabbing).
Ambiguous	The participant reports a *signal item** to be unclear or neutral, or 'does not know' where to place the card.
From previous experience	The participant mentions a previous experience with the *signal item**.

**Signal item = any singular signal color, symbol, or word*

Table 2. Qualitative content analysis themes and their definitions.

to work with at a time, starting from the most safe item to the most dangerous item. The final card placements were analyzed on Microsoft Excel, organized individually by colors, symbols and words, and the participant groups. We calculated the median rank of each signal item and placed them in increasing rank order for each category (e.g., color). We numbered the overall ranks from 1 to 20, by ordering the items from the 3 categories sequentially. Responses are summarized using box and whisker plots (discussed later in Figure 2), which visually compare the results from child and adult participants. We conducted inferential statistics using SPSS [23].

Qualitative Analysis Approaches

We applied content analysis methodology [11, 26, 54] to the qualitative data. In preparation, the primary researcher made sense of the whole dataset by reading the transcripts several times. By using an inductive approach, the primary researcher openly coded interview responses, created a coding sheet, grouped the data, and reduced the number of categories by combining similar headings into broader categories, and further refined the categories and sub-categories through abstraction. We then identified conceptual thematic mind maps for signal colors, symbols, and words. A thematic mind map is a tool to visualize and organize themes and sub-themes in qualitative analysis [48]. Using these mind maps, we identified 7 major themes describing users' perceptions (Table 2).

Using NVivo software [24], the primary researcher coded all card categorization and ranking response transcripts that included think-aloud commentary explaining participants' choices, and conducted analysis to further refine the themes. A research assistant independently coded 20% of the transcripts (transcripts for 5 children and 5 adults) based on the codesheet generated by the primary researcher. After coding was complete, the two researchers met and discussed their results. If new themes were discovered by the secondary researcher, the researchers discussed whether to include the new theme in the analysis. A Cohen's Kappa (k) test showed strong agreement between the two researchers' analysis of children's (k=0.88, 95% CI: 0.56 to 1.00, $p<0.005$), and of adults' activity transcripts (k=0.92, 95% CI: 0.63 to 1.00, $p<0.005$).

In the children's study, we extracted 572 excerpts for colors, 458 for symbols, and 454 for words. For adults, we extracted 1038 excerpts for colors, 762 for symbols, and 708 for words. These excerpts were coded under 7 major themes that we identified during the content analysis to describe participants' perception of the severity of hazard for each item and to explain their rationale for the placement of the cards. There may be multiple excerpts per participant and these may fall across different themes. Themes are not mutually exclusive and, therefore, one excerpt may be coded under multiple themes.

For the post-test interview, the primary researcher solely analyzed the data and tabulated the results since the data was straightforward and needed little interpretation.

FINDINGS

Both children and adults had similar notions about which signal items indicate the most dangerous and safest situations. They expressed similar concepts shaping their risk perceptions of warnings. As summarized in Figure 2 and Table 3, children and adults had fairly similar rankings for the top 3 most dangerous and safest signal colors, symbols, and words. In Table 3, dark blue boxes represent complete match in rank (e.g., both user groups ranked `red` as the most dangerous color), and light blue boxes represent a partial match (e.g., both groups placed `maroon` in the top 3, but adults ranked it the second most dangerous while children ranked it as the third).

Both groups considered `red`, `skull`, and `fatal` as the most dangerous, and `green` and `happy face` as the safest. Adults determined `online` was the safest word, but children placed it third; children ranked `protect` as safest instead. Children had the most variability in the hazard ranking of `navy`, `open lock`, and `blocked`, while adults varied in their ranking of `pink` and `security`. The `police officer` symbol had the most divergent rankings for both groups.

Statistical Analysis

Given the type of data we had, the large number of ranking items, and relatively low sample size, it was difficult to identify applicable statistical tests. For completeness, we briefly include the results of our inferential statistics, but note that these should be interpreted in context of the qualitative data. Using Friedman tests, we found significant differences at $p<0.001$ within each of the 6 groups (child-color, child-symbol, child-word, adult-color, adult-symbol, adult-word),

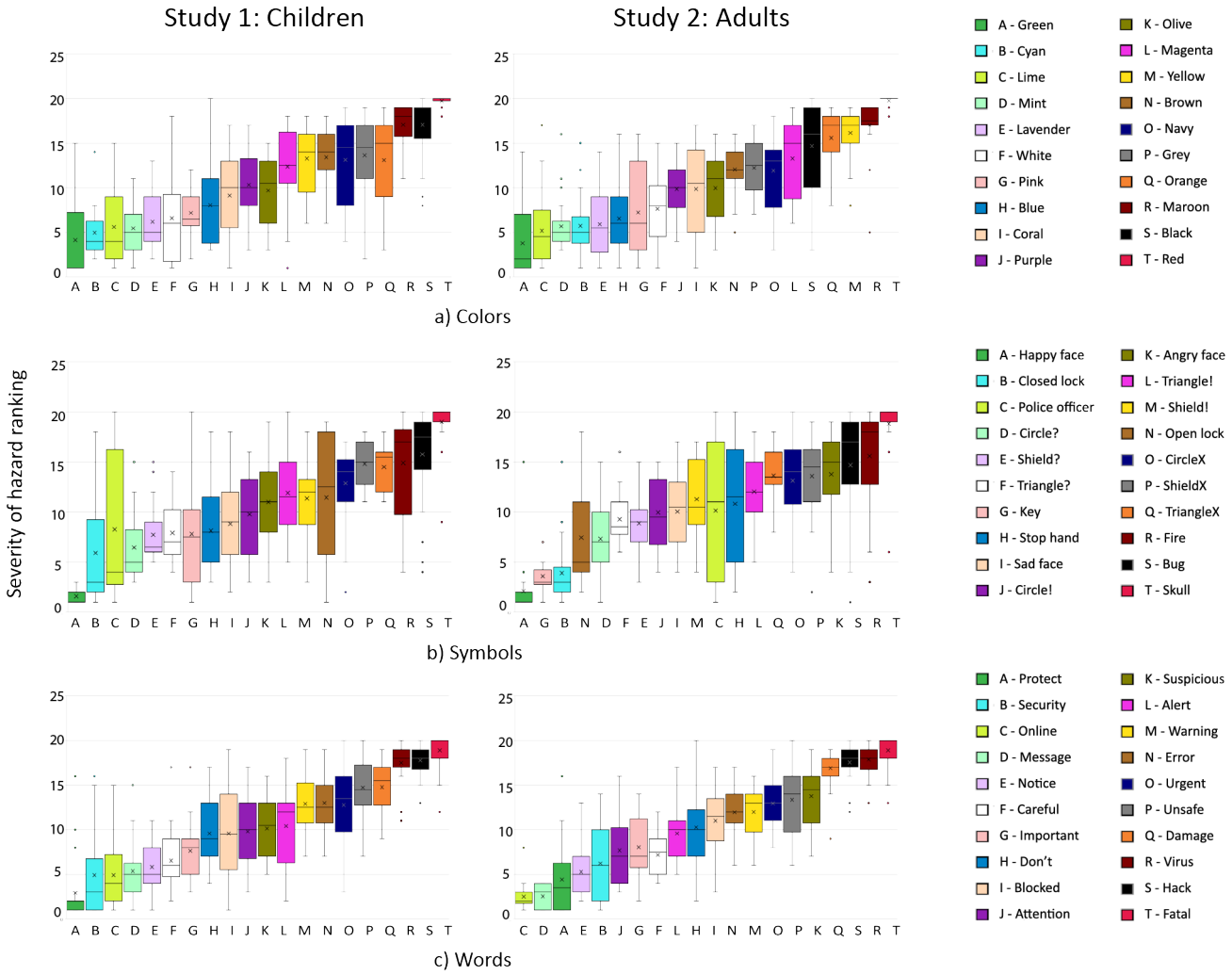

Figure 2. Children and adults' hazard ranking of a) colors, b) symbols, and c) words, where rank 1 = most safe, and 20 = most dangerous.

	SIGNAL COLORS				SIGNAL SYMBOLS				SIGNAL WORDS			
	Most Dangerous		Most Safe		Most Dangerous		Most Safe		Most Dangerous		Most Safe	
	Children	*Adults*	*Children*	*Adults*	*Children*	*Adults*	*Children*	*Adults*	*Children*	*Adults*	*Children*	*Adults*
1	Red	Red	Green	Green	Skull	Skull	Happy face	Happy face	Fatal	Fatal	Protect	Online
2	Black	Maroon	Cyan	Lime	Bug	Fire	Closed lock	Key	Hack	Virus	Security	Message
3	Maroon	Yellow	Lime	Mint	Fire	Bug	Police officer	Closed lock	Virus	Hack	Online	Protect

Table 3. Comparison of children and adults' top 3 rankings for most dangerous and safest signal colors, symbols, and words. *Dark blue* = complete match in rank between the two groups, and *Light blue* = partial match in rank, where both groups listed an item in the top 3, but in a different order.

indicating differences in perceived hazard of individual items within each group. Using Kendall's W tests, we found moderate to large effect sizes and agreement on the hazard ranking of items within each group (W-values between 0.47 and 0.72). Using Mann-Whitney tests with False Discovery Rate correction, we observed statistically significant differences between user groups for some words, where children found `online` and `message` more dangerous than adults, while adults found `suspicious` and `damage` more dangerous. Due to the large number of M-W comparisons, trends for colors and symbols approximated but did not reach statistical significance.

Signal Colors

For both user groups, darker shades were considered more dangerous while lighter, cooler, and pastel shades were considered safe. This is consistent with the literature [19, 22, 31]. Both groups showed a high level of agreement on the hazard ranking of `red`. Several participants explicitly mentioned that `red` was *"bad"* and `green` was *"good"* (n=5 children, 6 adults), which suggests that this concept may have been ingrained early through education, play, experience, or societal norms. Many participants mentioned 'contextual associations' with traffic signs and lights, where `red`, indicating *"stop"*, was dangerous and `green`, indicating *"go"*, was safe (n=5 children, 10 adults). Adults are accustomed to traffic lights, but children may learn from watching adults or through games such as *Red Light, Green Light* [46]. In this game, a person acting as a stoplight gives clear *red* or *green* signals to represent *stop* and *go*, encouraging children to form these associations.

Both groups considered `maroon` quite dangerous. Participants explained its ranking was due to its closeness with `red`:

> "[Maroon is] basically red, but a little more fancy." **C18**

> "[Maroon is a] combination and mix [of] red and black. Most dangerous color but also middle/neutral together. It is showing danger but not as strong as red." **A10**

Participants' perceived level of hazard for colors was highly dependent on individuals' subjective assessments. Colors with higher variability in their hazard ranking (e.g., `green`, `lime`, `white`, `pink`, `blue`, `coral`, `olive`, `yellow`, `navy`, `orange`) also showed high variability in individuals' color-emotion associations, personal preference, and past experience with each color [25]. In their study, Kaya and Epps [25] found that the intermediate hue *green-yellow* (similar to `lime`) elicited negative emotions associated with sickness and disgust. Similarly in our study, `green` and `lime` were predominantly considered safe and positive but some participants associated them with danger and negative emotions:

> "On PlayStation, there is a web browser, [and] sometimes random pop-ads come up. One time, [there] was a green ad [on] a small cybersecurity warning message. It just made me feel weird." **C22**

> "[Green] reminds of a traffic light. Since it's green, it doesn't make me feel unsafe. But you're still on the road, which you associate with danger; you need to be aware of your surroundings even if it's a green light." **A03**

> "[Lime is] a fruit and [it is] sour. Sour isn't good because it hurts." **C13**

> "In [the] Disney movies, all the villains have lime associated with [danger]. I don't think lime is truly an unsafe color, but if I had to rank it, it would be the least safe, in the middle." **A04**

We also observed differences between the two user groups. `black` was considered a top 3 dangerous color for children (rk=ranking=19) but not adults. Although `black` was still considered dangerous (rk=16), some adults said it was their *"favourite color"* (**A08**); children, however, found it *"scary"* (**C21**). Research on color-emotion associations show that children had negative reactions to *black* [5], but *black* elicited both negative (e.g., depression, fear, anger) and positive (e.g., richness, wealth, power) responses in adults [25].

In our research, children considered `yellow` to be somewhere in the middle on the danger scale (rk=13) because even though it was commonly seen on traffic signs and lights, `yellow` was also associated with the *"sun"* (**C10, C13**). This is consistent with a study that investigated children's emotional associations with colors, where they responded positively to bright colors like *yellow* [5]. In a general context, adults also associate *yellow* with positive emotions (e.g., happiness, excitement, sun, summer time) [25], but in the context of warning signs, they associate *yellow* with caution [19, 31]. In our study, adults ranked `yellow` among the most dangerous (rk=18).

Signal Symbols

Symbols that appear on other dangerous warnings (e.g., `shield X`, `circle X`, `triangle X`, `bug`), and those frequently observed on chemicals and hazardous material labels (e.g., `skull`, `fire`) were likely to be considered dangerous by both groups. On the other hand, symbols usually found on messages that indicate safety (e.g., `happy face`, `closed lock`, `key`) were considered safe by both. Children and adults showed a high level of agreement at the two extremes, `happy face` and `skull`, which suggests that these two symbols may be appropriate for cybersecurity warning messages.

Compound symbols with an 'icon within an icon', such as a `circle` with a `?`, were generally ambiguous. Children considered the symbol `circle ?` to be the most ambiguous (n=7), while `triangle ?` was most ambiguous for adults (n=8). Our results suggest that the `?` may be the main cause of the ambiguity in participants' perceptions:

> "[With circle ?], you are questioning yourself, 'Like what?"' **C21**

> "[Triangle ?] reminds you of [a] yield sign, something to be cautionary towards, like watch for falling rocks. [This is] more dangerous because it is now alert type thing rather than just a notification. [But] question mark makes it ambiguous." **A07**

For compound symbols, the inner symbol held more meaning than the outer symbol. All compound symbols with an `X` (e.g., `shield X`) were more dangerous than those with `!` (e.g., `shield !`). Finally, both groups believed that symbols with `?` (e.g., `shield ?`) were safest among the compound symbols.

For symbols associated with emotions like `angry face`, some adults believed them to be more effective for children. They thought that children would have an easier time determining arousal strength with emotive symbols than those requiring more knowledge and experience:

> "[Is this] yelling or yawning? I'm gonna assume it's yelling, and that's more negative in facial recognition. I think it would be more effective with children. A lot of these symbols are things I associated with experience or road signs and world experience. But children don't have that. Happy face, sad face or angry face are more effective for children because they're simplistic and [children] have come across them in [the] media." **A20**

Children and adults considered `happy face` to be the safest (*rk*=1) and most positive; `sad face` fell in the middle category (*rk*=9). Interestingly, while adults considered `angry face` dangerous (*rk*=17), children ranked it in the middle (*rk*=11) although opinions were mixed. Emotive symbols may be interpreted differently depending on the individual's subjective perception. For example, one child participant placed `angry face` in the safe category and explained:

> "Yelling face, it's not dangerous because some sites won't use these faces (smiley, sad, angry). These are kind of funny, they won't use it to get anyone's attention." **C11**

Although both groups had mixed feelings on `police officer`, children generally considered it safe (*rk*=3) and discussed this symbol in a positive light, while adults believed that it had a more negative connotation (*rk*=11):

> "Police - they usually help you with something dangerous. Security guard — it is secure." **C06**
>
> "[A police officer] can be safe and dangerous. It protects that website from hackers but if you say rude comments or inappropriate [things on the] website, the security guard or police officer can find you with your email. With a security guard, [it is] pretty much the same, but could be either dangerous or safe." **C12**
>
> "The police are monitoring the website. There might be illegal activity on the website, indicating that it is dangerous." **A06**
>
> "[Police officer or security guard is] supposed to protect you, but at the same time, it can be threatening, saying that there's imminent danger, or a possible threat." **A17**

Interestingly, while both groups associated the `closed lock` with safety, opinions varied for the `open lock`. Given that a `closed lock` symbol is a common security indicator [13], it would make sense for users to assume the opposite for the `open lock`. However, adults found `open lock` to be safe (*rk*=4), while most children placed it in the middle and dangerous categories (*rk*=14). We found the differences in both groups' associations of `open lock` with physical security metaphors [42]. For example, the `open lock` may suggest that it is safe to proceed:

> "[Open lock means that] the site is open to everyone, open source basically. I don't believe it would be dangerous if it is open source." **C13**
>
> "[Open lock means] unlocked, access, the password was correct." **C18**
>
> "When you see a padlock [and] you see a little open[ing], it makes me feel better than a closed lock...I used to play games and [when] you unlock achievements, the padlock opens." **A03**
>
> "Open lock is not dangerous, you can go ahead because it is open. It is safe so you can use it." **A10**
>
> "Open lock [means it is] unlocked, you succeeded by unlocking something. You put in your password. I don't know where I've seen this but I am thinking about my Apple ID." **A21**

Some adults talked about the `open lock` in comparison to the `closed lock`. They mentioned that the `open lock` was less safe, but that did not necessarily mean the symbol was dangerous because users still have the option to lock it:

> "Something is unlocked, but it can be locked, more or less. [You are] not protected, but it's more of a safety warning [so] you can lock it." **A02**
>
> "Open lock [is] commonly used in computer or cybersecurity [contexts]. Since [it is] unlocked, someone or something can easily hack it, [and] it might not be a protected network. There's still the possibility of lock[ing] it if you need to." **A17**

On the other hand, children are used to seeing things that are locked. For example, some kids have to wait for adults to open doors or for their parents to unlock the screen on their tablets. When these children run into things that are unlocked without their parents' permission, it may raise suspicion:

> "[When] you go [online] to see your email, [it is] something private that's just for you. [Open lock] shows you that someone else saw it or it's open to other people. It's a public thing, not private, so [it is] not safe just for you anymore." **C12**
>
> "Unlocked lock [means] the website is insecure." **C14**
>
> "Your computer is unlocked, anybody can get in." **C21**

These results suggest that the intended binary relationship could be easily misinterpreted for the lock symbol:

> "You don't really know if [the open lock] means something good or bad. With my lock code, if it unlocks, [that] means I can get in. But [it can] also mean someone else can get in." **A19**

Signal Words

Both groups agreed on the most dangerous words: `virus`, `hack`, and `fatal`. Participants discussed `virus` and `hack` using metaphors in the context of cybersecurity. They mentioned that when they saw these words on warnings, it made them feel like their computers were *"infected or contaminated"* (**C14**, **A01**) and *"being taken over"* (**C06**, **A06**). Children and adults perceived `fatal` as having a negative connotation associated with *"death"* (**C19-21, A02-3, A06**). This implies that when used on cybersecurity warnings, these three signal words may be highly effective in communicating a high degree of risk.

Both children and adults believed that the word `blocked` could easily be misinterpreted because it could insinuate that the application they are using may be either safe or dangerous. For example, a safer environment may be created when users' access is removed altogether from dangerous things:

> "[It is] not dangerous if something is blocked. If you search something, it won't even come up. On Google, it may just say access blocked, so it's trying to keep you safe." **C12**

On the other hand, participants believed that being *blocked* could indicate danger:

> "[The] site is blocked, which means it's probably dangerous. No one wants you to go into it." **C13**

> "Your computer might have blocked a virus or potential damage to your computer. It blocked it but you should be aware of the potential damage that could happen to your device." **A21**

There was higher variability in children's risk perception of words like `damage` and `suspicious` compared to adults. Some children placed `damage` in the middle category and explained that something could be damaged *"a little bit"* (**C20**, **C22**). Adults placed `suspicious` in the dangerous category (*rk*=16), but the majority of children placed it in the middle (*rk*=11) because they associated the word with *potential* danger rather than an actual hazard (*n*=5).

Post-Test Interview

All participants provided reasonable definitions of warning messages. Based on Cranor's [10] classification, both groups primarily defined warning messages as *warning dialogs*, which alert users to take immediate action to avoid a threat.

Both groups had similar attitudes toward cybersecurity warnings. Most participants viewed warnings as *both* positive and negative. We found that those who viewed warnings *negatively* generally misunderstood the purpose of warnings and associated them with malicious intentions such as fake, phishing messages that give viruses, scare, overwhelm, and desensitize users. Consistent with the findings by Fagan *et al*. [12], the general negative attitudes associated with warnings stemmed from users' negative past experiences, such as messages that are *"annoying"* (e.g., interrupting users' activities).

Most participants reported *reading* the warning messages they encountered. A significant portion reported that they try to ignore the warning and continue with their primary activity if possible, highlighting that security is a secondary task [49].

Most children reported that they showed cybersecurity warnings to someone else. Children generally reported to *adults* (e.g., a parent, older sibling, teacher) rather than friends, while a few adults talked to someone more *"technology-savvy"* (e.g., *family* members, *friends*, *professional help*). Adults who did not report to anyone were confident in dealing with the warnings by themselves, and others came to them for help.

DISCUSSION

Key Findings and Contribution

In their study with older adults, Garg *et al*. [17] noted additional constraints when designing for a specific population; we believe the same applies for children. Children are increasingly exposed to online security threats [30,35,36,47]. We aim to understand children's unique risk perceptions and how they respond to the different components of cybersecurity warnings so that we can better match the design of warnings to their needs. While some of our findings confirm 'common sense knowledge', we believe that *(1)* having empirical data showing that these are valid, especially for children, *(2)* identifying ambiguities in commonly used items, and *(3)* exploring 'why' these perceptions exist, are valuable contributions.

Aligning with the literature [2, 19, 22, 31, 43], our findings confirm that both children and adults perceive `red`, `skull`, and `fatal` as dangerous, and `green` and `happy face` as safe. This suggests similarities in how both children and adults interpret some signal items. We found high agreement on certain signal items, and identified these as the least ambiguous. To the best of our knowledge, prior work had not identified the ambiguity of the `open lock` and `police officer` symbols. Our results demonstrate that both children and adults had mixed interpretations of these items. While these symbols may still be viable in warnings in combination with other design parameters, their ambiguity is a concern.

Previous studies with children examined and evaluated warning designs [16, 37, 53]. Our research extends this work by exploring *why* these perceptions exist, particularly because children and adults are fundamentally different in their psychology and mental models [55, 56]. We observed differences pertaining to personal preferences for colors, attitudes towards signal items (e.g., children generally discussed `police officer` in a more positive light than adults), and the simplicity of the rationale behind the card placements (e.g., a few children gave one-word responses without providing further explanation even when probed). Individual user differences affect how users understand and respond to security communications [10], and we found that these differences also affect interpretations of the individual design parameters.

Design Implications For Children

Our research provides preliminary data on children's perception of signal colors, symbols, and words in the context of cybersecurity warnings. Reflecting on our findings in light of the literature, we discuss implications for warning design. These should be explicitly tested for clarity in future work, but they offer promising directions.

1. Be clear. Simple and basic signal colors, symbols, and words should clearly and appropriately communicate the level of hazard for children. We recommend designers to use the signal items at the extreme ends of the hazard ranking scale since they have lower likelihood of being misinterpreted by users. For example, the items from Table 3 were the most clear of the set we tested and would be appropriate for use. Many cybersecurity warnings contain technical terms and computer jargon that are difficult for users to understand [8]. Some

participants mentioned the importance of keeping the words simple because the general population does not understand jargon or error codes (**A02, A13, A18**). This idea particularly applies to children, who may have less advanced vocabulary.

2. Eliminate ambiguity. Ambiguous signal items may be misinterpreted or interpreted in multiple ways. Our results show that the binary relationship between `open lock` and `closed lock` can be unclear. Although `closed lock` clearly conveyed 'secure', both groups had mixed interpretations of the `open lock`. Similarly, while children clearly identified `police officer` as secure, adults had mixed feelings. The word `blocked` was also interpreted by some participants as secure and by others as dangerous. Furthermore, participants had difficulty ranking compound symbols; they interpreted the components separately and prioritized the inner symbol. We suggest designers disregard items that may cause confusion and use items unambiguous to both groups, where children and adults' interpretations align. We particularly note that designers should reconsider the lock symbol as a security indicator given its ambiguity. We also suggest avoiding compound symbols since they seemed particularly prone to difficulty.

3. ***Explore adult-child interaction.*** Our results echo existing findings that children often report warnings to adults and largely rely on their parents for support [27, 28, 55, 56]. When children encounter something unknown, they are dependent on adults. Some children suggested that warnings should include child-appropriate information and communicate in a way that makes sense to children without causing undue fear:

> "Explain it in a kid version. Something I could understand, and don't make it too scary." **C21**

Designers should further explore this adult-child interaction in the cybersecurity context. We suggest the possibility of providing a *"kid version"* for warnings. For instance, providing a 'child' warning that suggests getting a trusted adult, with an option to convert to the 'adult' warning when help arrives; or enabling the browser or operating system to be in 'child' mode and displaying appropriate child-friendly warnings (e.g., as an overlay that translates existing adult warnings for applications or websites that do not have this functionality included).

4. ***Combine design parameters.*** Both groups found it more difficult to categorize colors than symbols and words. They emphasized that color by itself did not give enough information to establish context for warnings. This suggests that colors may be more effective in communicating risk when used in tandem with other design parameters. This was also evident from the card sorting. Most participants described colors in association with symbols and words. For example, `red` was discussed using symbols like `fire`, *"stop sign"* and *"X"*, and words like `attention` and `urgent`. Children mentioned that symbols were the least difficult to categorize out of the three design parameters because they had 'previous experience' seeing them (**C01, C11**). Similarly, research on warning labels [40] found that users were much more likely be pay attention to messages with symbols than those relying solely on text. Further exploration on how to best combine design parameters to convey risk to children would be beneficial.

LIMITATIONS AND FUTURE WORK

We opted for a methodology that enabled us to test many items. Participants may respond differently when faced with these signal items as part of an actual cybersecurity warning. Our results can inform follow-up studies by providing a subset of signal items that are most likely effective.

The post-test interview analysis was completed by one researcher since this data was straightforward and needed little interpretation. Although we were careful, there may be some bias from the single perspective.

We attempted to cover a representative range of signal items, but it is possible that others may be more effective. Our results can only compare the set of items we had to each other.

We did not ask participants to quantify the arousal strengths, so we do not know the exact difference between items. Instead, we can say that we have produced ordinal scales of signal colors, symbols, and words from *safest* to *most dangerous*. Since this was a first attempt at scaling the level of hazard for these signal items, future studies could test replicability and generalizability of these scales to establish more robust scales.

We focused on two user groups, children and adults. Although we recruited our participants through various methods, we acknowledge that our sample was fairly homogeneous in terms of socio-economic status. This may have impacted their interpretation of the signal items. Future studies may benefit from considering participants from varying demographics such as age, gender, and cultural and economic background.

CONCLUSION

Although much research has been conducted on warnings with adults, their responses may not accurately reflect the needs of children. We wanted to address this research gap and work towards cybersecurity warnings that effectively communicate risk to children. We conducted two user studies and uncovered similarities and differences between children and adults' perception of signal colors, symbols, and words. Through interviews, we identified concepts and associations that shaped children and adults' risk perceptions. We discovered potential concerns with some signal items that are widely used as security indicators, such as the `open lock`, `police officer`, and compound symbols that have an 'icon within an icon'. The good news is that existing cybersecurity warnings may still be usable for children with some minor tweaking. We suggest security practitioners and designers to use a subset of signal items that are least ambiguous for both groups (e.g., `red`, `skull`, and `fatal` to convey danger, and `green`, `happy face`, and `protect` to convey safety), and to keep in mind the individual differences that are outlined in this research.

ACKNOWLEDGMENTS

We thank the participants and reviewers for their time. We also acknowledge funding from the Ontario Ministry of Research, Innovation and Science Early Researcher Award, the NSERC Discovery Grant, and the Canada Research Chairs program.

REFERENCES

[1] Devdatta Akhawe and Adrienne P. Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Proceedings of the 22nd USENIX Security Symposium (USENIX '13)*. USENIX Association, Washington, D.C., USA, 257–272. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

[2] T. S. Amer and Jo-Mae B. Maris. 2007. Signal Words and Signal Icons in Application Control and Information Technology Exception Messages – Hazard Matching and Habituation Effects. *Journal of Information Systems* 21, 2 (2007), 1–25. DOI: http://dx.doi.org/10.2308/jis.2007.21.2.1

[3] Bonnie B. Anderson, C. Brock Kirwan, Jeffrey L. Jenkins, David Eargle, Seth Howard, and Anthony Vance. 2015. How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2883–2892. DOI: http://dx.doi.org/10.1145/2702123.2702322

[4] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. 2013. *Warning Design Guidelines*. Technical Report CMU-CyLab-13-002. CyLab, Carnegie Mellon University. http://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13002.html

[5] C. J. Boyatzis and Ramani Varghese. 1994. Children's Emotional Associations with Colors. *The Journal of Genetic Psychology* 155, 1 (1994), 77–85.

[6] Curt C. Braun, Paul B. Mine, and N. Clayton Silver. 1995. The Influence of Color on Warning Label Perceptions. *International Journal of Industrial Ergonomics* 15, 3 (1995), 179–187. DOI: http://dx.doi.org/10.1016/0169-8141(94)00036-3

[7] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. 2014. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, USA, 105–111. https://www.usenix.org/conference/soups2014/proceedings/presentation/bravo-lillo

[8] Cristian Bravo-Lillo, Lorrie F. Cranor, Julie S. Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26. DOI:http://dx.doi.org/10.1109/MSP.2010.198

[9] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie F. Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, 1–12. DOI: http://dx.doi.org/10.1145/2501604.2501610

[10] Lorrie F. Cranor. 2008. A Framework for Reasoning About the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC '08)*. USENIX Association, Berkeley, CA, USA, 1–15. http://dl.acm.org/citation.cfm?id=1387649.1387650

[11] Satu Elo and Helvi Kyngäs. 2008. The Qualitative Content Analysis Process. *Journal of Advanced Nursing* 62, 1 (2008), 107–115. DOI: http://dx.doi.org/10.1111/j.1365-2648.2007.04569.x

[12] Michael Fagan, Mohammad M.H. Khan, and Nhan Nguyen. 2015. How does this message make you feel? A study of user perspectives on software update/warning message design. *Human-centric Computing and Information Sciences* 5, 1 (15 Dec 2015), 1–26.

[13] Adrienne P. Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa E. Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Proceedings of 12th Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX Association, Denver, CO, USA, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

[14] Canadian Centre for Occupational Health and Safety. 2015. WHMIS 2015 – Labels. https://www.ccohs.ca/oshanswers/chemicals/whmis_ghs/labels.html. (2015).

[15] Canadian Centre for Occupational Health and Safety. 2016. WHMIS 2015 Fact Sheets. https://www.ccohs.ca/products/publications/whmis_ghs/. (09 2016).

[16] Jana Fruth, Ronny Merkel, and Jana Dittmann. 2011. Security Warnings for Children's Smart Phones: A First Design Approach. In *Proceedings of the 12th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS '11)*. Springer-Verlag, Berlin, Heidelberg, Germany, 241–243. http://dl.acm.org/citation.cfm?id=2046108.2046146

[17] Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. 2012. Risk Communication Design: Video vs. Text. In *Proceedings of the 12th International Conference on Privacy Enhancing Technologies (PETS '12)*. Springer-Verlag, Berlin, Heidelberg, 279–298. DOI: http://dx.doi.org/10.1007/978-3-642-31680-7_15

[18] Debra L. Gelman. 2014. *Design For Kids: Digital Products for Playing and Learning*. Rosenfeld Media, Brooklyn, NY, USA.

[19] L.J. Griffith and S. David Leonard. 1997. Association of colors with warning signal words. *International Journal of Industrial Ergonomics* 20, 4 (1997), 317–325. DOI: http://dx.doi.org/10.1016/S0169-8141(96)00062-5

[20] Elizabeth Hellier, Kirsteen Aldrich, Daniel B. Wright, Denny Daunt, and Judy Edworthy. 2007. A Multi Dimensional Analysis of Warning Signal Words. *Journal of Risk Research* 10, 3 (2007), 323–338. DOI: http://dx.doi.org/10.1080/13669870601066963

[21] Elizabeth Hellier, Daniel B. Wright, Judy Edworthy, and Stephen Newstead. 2000. On the stability of the arousal strength of warning signal words. *Applied Cognitive Psychology* 14, 6 (2000), 577–592. DOI: http://dx.doi.org/10.1002/1099-0720(200011/12)14:6<577::AID-ACP682>3.0.CO;2-A

[22] Linda Holtzschue. 2017. *Understanding Color: An Introduction for Designers* (5th ed.). Wiley, Hoboken, NJ, USA.

[23] IBM. 2019. IBM SPSS software. https://www.ibm.com/analytics/spss-statistics-software. (2019).

[24] QSR International. 2018. What is NVivo? https://www.qsrinternational.com/nvivo/what-is-nvivo. (2018).

[25] Naz Kaya and Helen H. Epps. 2004. Color-emotion Associations: Past Experience and Personal Preference. In *AIC 2004 Color and Paints, Proceedings of the Interim Meeting of the International Color Association (AIC '04)*. Brazilian Color Association, Porto Alegre, Brazil, 31–34. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.616.6634&rep=rep1&type=pdf

[26] Klaus Krippendorff. 2004. *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Sage Publications, Thousand Oaks, CA, USA.

[27] Priya Kumar, Shalmali M. Naik, Utkarsha R. Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 64:1–64:21. DOI:http://dx.doi.org/10.1145/3134699

[28] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 307:1–307:13. DOI: http://dx.doi.org/10.1145/3290605.3300537

[29] Kaspersky Lab. 2017. *Kaspersky Security Bulletin: Overall Statistics for 2017*. Technical Report. Kaspersky Lab. https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Statistics-PR-1045.pdf

[30] Elmer Lastdrager, Inés C. Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-phishing Training for Children?. In *Proceedings of the 13th USENIX Conference on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 229–239. http://dl.acm.org/citation.cfm?id=3235924.3235943

[31] S. David Leonard. 1999. Does color of warnings affect risk perception? *International Journal of Industrial Ergonomics* 23 (1999), 499–504.

[32] Qingguo Ma, Xiaoxu Bai, Guanxiong Pei, and Zhijiang Xu. 2018. The Hazard Perception for the Surrounding Shape of Warning Signs: Evidence From an Event-Related Potentials Study. *Frontiers in Neuroscience* 12, 824 (2018), 1–8. DOI: http://dx.doi.org/10.3389/fnins.2018.00824

[33] Common Sense Media. 2019a. What's age-appropriate for 10- to 12-year-olds? https://www.commonsensemedia.org/about-us/our-mission/about-our-ratings/10-12. (2019).

[34] Common Sense Media. 2019b. What's age appropriate for a 10-year-old? https://www.commonsensemedia.org/about-us/our-mission/about-our-ratings/10. (2019).

[35] MediaSmarts. 2014a. Internet safety tips by age: 11-13. http://mediasmarts.ca/tipsheet/internet-safety-tips-age-11-13. (2014).

[36] MediaSmarts. 2014b. Internet Safety Tips by Age: 8-10. http://mediasmarts.ca/tipsheet/internet-safety-tips-age-8-10. (2014).

[37] Wiebke Menzel, Sven Tuchscheerer, Jana Fruth, Christian Kraetzer, and Jana Dittmann. 2012. Design and evaluation of security multimedia warnings for children's smartphones. In *Proceedings of the SPIE 8304, Multimedia on Mobile Devices 2012; and Multimedia Content Access: Algorithms and Systems VI (SPIE '12)*. Society of Photo-Optical Instrumentation Engineers (SPIE), Washington, USA, 1–9. DOI: http://dx.doi.org/10.1117/12.908026

[38] Anca Micheti, Jacquelyn Burkell, and Valerie Steeves. 2010. Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand. *Bulletin of Science, Technology & Society* 30, 2 (2010), 130–143. DOI:http://dx.doi.org/10.1177/0270467610365355

[39] Ministry of Transportation. 2017. The Official Ministry of Transportation Driver's Handbook: Traffic Signs and Lights. https://www.ontario.ca/document/official-mto-drivers-handbook/traffic-signs-and-lights. (1 2017).

[40] Michelle O'Hegarty, Linda L. Pederson, David E. Nelson, Paul Mowery, Julia M. Gable, and Pascale Wortley. 2006. Reactions of Young Adult Smokers to Warning Labels on Cigarette Packages. *American Journal of Preventive Medicine* 30, 6 (2006), 467–473. DOI:http://dx.doi.org/https://doi.org/10.1016/j.amepre.2006.01.018

[41] Qualtrics. 2018. Online Survey Software. https://www.qualtrics.com/research-core/survey-software/. (2018).

[42] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le C. Wang, and Konstantin Beznosov. 2011. A Brick Wall, a Locked Door, and a Bandit: A Physical Security Metaphor for Firewall Warnings. In *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS '11)*. ACM, New York, NY, USA, 1–20. DOI: http://dx.doi.org/10.1145/2078827.2078829

[43] Mario Silic, Dianne Cyr, Andrea Back, and Adrian Holzer. 2017. Effects of Color Appeal, Perceived Risk and Culture on User's Decision in Presence of Warning Banner Message. In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS '17)*. ScholarSpace / AIS Electronic Library (AISeL), Hawaii, USA, 1–10. DOI: http://dx.doi.org/10.24251/HICSS.2017.065

[44] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie F. Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the 18th Conference on USENIX Security Symposium (SSYM '09)*. USENIX Association, Berkeley, CA, USA, 399–416. http://dl.acm.org/citation.cfm?id=1855768.1855793

[45] Amanda Third, Delphine Bellerose, Juliano D. De Oliveira, Girish Lala, and Georgina Theakstone. 2017. *Young and Online: Children's Perspectives on Life in the Digital Age (The State of the World's Children 2017 Companion Report)*. Western Sydney University, Sydney, SNW, Australia. DOI: http://dx.doi.org/10.4225/35/5a1b885f6d4db

[46] Shauna Tominey and Megan Mcclelland. 2011. Red Light, Purple Light: Findings From a Randomized Trial Using Circle Time Games to Improve Behavioral Self-Regulation in Preschool. *Early Education and Development* 22 (2011), 489–519. DOI: http://dx.doi.org/10.1080/10409289.2011.574258

[47] United Nations Children's Fund (UNICEF). 2018. *The State of the World's Children 2017: Children in a Digital World*. UNICEF, New York, NY, USA. DOI: http://dx.doi.org/10.18356/d2148af5-en

[48] Johannes Wheeldon and Jacqueline Faubert. 2009. Framing Experience: Concept Maps, Mind Maps, and Data Collection in Qualitative Research. *International Journal of Qualitative Methods* 8, 3 (2009), 68–83. DOI: http://dx.doi.org/10.1177/160940690900800307

[49] Alma Whitten and J.D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium (SSYM '99)*. USENIX Association, Berkeley, CA, USA, 169–184. http://dl.acm.org/citation.cfm?id=1251421.1251435

[50] Michael S. Wogalter. 2006a. *Handbook of Warnings* (1st ed.). Lawrence Erlbaum Associates, Mahwah, NJ, USA, Chapter Communication-Human Information Processing (C-HIP) Model, 51–61.

[51] Michael S. Wogalter. 2006b. *Handbook of Warnings* (1st ed.). Lawrence Erlbaum Associates, Mahwah, NJ, USA, Chapter Purposes and Scope of Warnings, 3–9.

[52] Michael S. Wogalter, Vincent C. Conzola, and Tonya L. Smith-Jackson. 2002. Research-based guidelines for warning design and evaluation. *Applied Ergonomics* 33 (2002), 219–230. http://www.who.int/fctc/guidelines/ArtElevenWogalterNine.pdf

[53] Helen Zaikina-Montgomery and N. Clayton Silver. 2018. An examination of icons, signal words, color, and messages in warnings for children on the Internet. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (2018), 251–255. DOI: http://dx.doi.org/10.1177/1541931218621058

[54] Yan Zhang and Barbara M. Wildemuth. 2009. *Applications of Social Research Methods to Questions in Information and Library Science* (2nd ed.). Libraries Unlimited, Santa Barbara, CA, USA, Chapter Qualitative Analysis of Content, 318–329.

[55] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13 (2017), 10–18. DOI: http://dx.doi.org/10.1016/j.ijcci.2017.05.001

[56] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the 15th International Conference on Interaction Design and Children (IDC '16)*. ACM, New York, NY, USA, 388–399. DOI: http://dx.doi.org/10.1145/2930674.2930716

[57] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I Make Up a Silly Name': Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 106:1–106:13. DOI: http://dx.doi.org/10.1145/3290605.3300336