CHILDREN AND ADULTS' PERCEPTION OF SIGNAL COLOURS, SYMBOLS, AND WORDS IN THE CONTEXT OF CYBERSECURITY WARNINGS

by
Rebecca Jeong

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF ARTS

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
January, 2019

Abstract

Research has shown that online security warnings are frequently ignored or misinterpreted by even experienced adult users. Children may be particularly vulnerable because they are not always aware of the risks associated with online threats. Existing work relating to cybersecurity warnings has been done with adults and there are few recommendations for children. We explore this research gap through two user studies with 22 children aged 10-12 years old and with 22 adults. We compare children and adults' perception of warning design parameters (signal colours, symbols, and words) in the context of cybersecurity warnings. Our findings suggest that while there are many similarities in how both groups interpret the signal items, differences exist which should be taken into consideration when designing for children. We adapt existing warning design guidelines by Bauer *et al.* to provide recommendations for warnings that effectively communicate risk to children.

Acknowledgements

First, I would like to give my thanks to my wonderful supervisor, Sonia Chiasson, for her guidance, patience, and support throughout my journey at Carleton. I am forever grateful for your mentorship and am truly inspired by your dedication to your students. Thank you for providing me with the invaluable opportunity to work with you. Most of all, I appreciate the weekly updates on your adventures with the cats, they always cheered me up!

Special thanks to the members of my defence committee, Elizabeth Stobert and Vicky McArthur, and Kasia Muldner for chairing my defence. I appreciate all your guidance and feedback, which greatly helped me to improve this thesis.

Many thanks to Lois Frankel for her encouragement and the opportunity to begin my journey in HCI and UX. Thanks to Anthony Whitehead for his inspiration, he will always be remembered.

I would like to thank all the amazing members of the CHORUS laboratory - Daniela, Khadija, Sana, Michael, Reham, Yomna, Jessica, Hala and Fiona. Big thanks to my fabulous friends - Anis, Sanaz, Nour, Aya, Misha, Ryo, Justin and Lisa. Thank you guys for believing in me and assisting me throughout the process.

To my family - my loving parents Youngjin and Myounghwa, my beautiful sister Lydia, and wonderful Felicia and Marshall. Thank you for all your prayers, love, and support.

To my Eddie, thank you for loving me, being there for me, and putting a smile on my face everyday. I could not have done this without you.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

According to Kaspersky Lab [35], 29.4% of user computers underwent online malware attack at least once in 2017. Canada was among the top 10 countries where online resources contained malware [35]. Cybersecurity warnings are intended to help users protect their data and their computers from these and other threats [9]. However, research has shown that online security and privacy warnings are frequently ignored or misinterpreted by even experienced adult users [1,9]. Even when risk is imminent, many studies indicate that people do not read, understand, or heed to computer warnings [1,9,55].

Therefore, improving security warnings is imperative in human-computer interaction to properly alert users of existing or imminent threats, and encourage users to take appropriate security measures [9]. The human-in-the-loop (HITL) security framework by Cranor [13] suggests that warnings designed to communicate risk more effectively can help mitigate threats. Warnings consist of several components including signal colours, symbols, and words. These design parameters cue users to the severity of the threat and help determine how much attention and credibility users will allocate to the warnings. To be effective, the level of hazard must be appropriately conveyed. In other words, the level of hazard intended by the designer must match the level of hazard perceived by the user [3].

While studies have been conducted to examine warning design for adults [3,16,25–27,36,64], there is little data to establish recommendations for children. It is unclear whether children interpret the design parameters in the same way as adults.

Children are one of the fastest growing populations online worldwide: 99% of Canadian students between the ages of 9 to 17 years old (Grade 4 to 11) access the Internet outside of school [54]. Similarly, Common Sense Media [39] conducted a

survey in 2017, which reported that online viewing accounted for 25% of TV and video time for American children under the age of 8, and 22% of children between the ages of 5 to 8 years old often or sometimes played online social games such as Animal Jam and Minecraft [39]. Almost all American children under the age of 8 (98%) were exposed to a mobile device at home, which allowed them to easily go online [39]. Another survey conducted in 2010 found that half of children aged 6 to 13 owned a mobile phone in Germany [42].

When we shift our focus from adults to children, privacy and security issues become more complicated [67]. Children may be particularly vulnerable because they are not always aware of the risks associated with online threats [67] nor understand the consequences of their actions. To help children make safer choices online, we must first be able to communicate in ways that are meaningful to them. As a starting point, this thesis explores children's interpretation of different design parameters for cybersecurity warnings. We also observe adults' perspective because current cybersecurity warnings are typically designed for adult users [22, 42] and their data can serve as a baseline.

1.2 Research Questions

This study explores an overall research question:

> "How do children and adults compare in their perceptions and understanding of signal colours, symbols, and words in the context of cybersecurity warning messages?"

Our main research question was guided by three sub-research questions:

1. **RQ1) Children's perception of severity of hazard**: How do children comprehend and perceive the severity of hazards associated with warning design parameters (signal colours, symbols, and words)?
2. **RQ2) Adults' perception of severity of hazard**: How do adults comprehend and perceive the severity of hazards associated with warning design parameters (signal colours, symbols, and words)?

3. **RQ3) Comparison**: How do the two groups compare?

1.3 Contributions

This research contributes to the literature on children and cybersecurity warnings. Our studies identify similarities and differences between children and adults' perception of warning design parameters. We make the following four contributions:

1. We provided data on children and adults' perceived level of hazards for signal colours, symbols, and words.

2. We identified how children and adults compare in their perceptions of, previous experiences with, and expectations for cybersecurity warning design parameters.

3. We identified some concepts and associations that shaped children and adults' risk perceptions, and helped them to determine what is dangerous or safe when it comes to signal colours, symbols, and words.

4. We adapted the warning design guidelines by Bauer *et al.* [5] to provide recommendations to consider when developing cybersecurity warning messages for children.

1.4 Thesis Outline

In *Chapter 2*, we give a background on children and cybersecurity warnings using the human-in-the-loop (HITL) security framework. In *Chapter 3*, we describe the methodology for our user studies with children and adults. We present the findings in *Chapters 4 and 5*. In *Chapter 6*, we compare the two studies. In *Chapter 7*, we discuss the implications of our findings, limitations of our studies and future research directions.

Chapter 2

Background

In this chapter, we discuss warning messages in a cybersecurity context. We address some of the dimensions in the *human-in-the-loop* (HITL) security framework [13], including the types of communication that are relevant to security warnings, the human receiver, and the desired behaviour from effective security warnings. We end the chapter by identifying the research gaps pertaining to children that we will address throughout the thesis. For definitions, refer to Appendix A.

2.1 Warnings

Warnings are a type of communication designed to prevent people from harm [5,9,62]. Warnings can include information on the presence of hazards and instructions on how to avoid them [9, 25, 63], so that they not only alert users of existing or imminent threats but also remind users or change user behaviour [9].

Warnings are part of people's daily lives. They are everywhere and we encounter them in various situations [3] regardless of whether we take notice. Warnings can be observed on road signs while driving, on warning labels placed on household chemicals used for cleaning, or while browsing online.

In cases where secure systems cannot design out risk or completely protect users from harm, warnings are used as the next line of defense [1,4,9,13,55,63]. Sometimes, we cannot automate security-critical tasks and must rely on humans to make informed judgments [13]. In the past few decades, proper design and evaluation of warnings has been considered an important topic in usable security and other fields of human-computer interaction [64].

2.2 Human-in-the-Loop Framework

When software systems cannot rely on automated components alone to perform security-critical tasks, they turn to user judgment [9, 13].

Cranor [13] proposes the *human-in-the-loop* (HITL) security framework, which addresses the issue of where human reasoning should be employed in security decision making. This framework is based on the *communication-human information processing* (C-HIP) model developed by Wogalter [62] that describes security processing steps that users experience when they encounter warnings. The HITL framework guides security experts and designers to identify and reduce the occurrence of human-related security failures when they interact with software systems. Figure 2.1 summarizes the sequential stages and information processing of the HITL security framework.

In the context of cybersecurity and for the purpose of this research, we use the definition of warning from the HITL framework, which includes five different types of communications relevant to security tasks [13]:

1. *Warning dialogs*: alert users to take immediate action to avoid a threat (e.g., anti-phishing, expired SSL certs)

2. *Notices*: provide users information and characteristics of entity or object (e.g., privacy polices, SSL certs)

3. *Status indicators*: inform users about system status or the risk condition (e.g., taskbar and menu bar indicators about bluetooth, virus software up-to-date, file permissions)

4. *Training*: teach users about security threats and how to respond to them (e.g., tutorials, games, instruction manuals, web sites, emails, seminars, courses)

5. *Policies*: inform users about system or organizational policies (e.g., ISP terms of service, employee handbook, password policy, policy on encrypting documents)

Security communications can be classified into more than one type of communications (e.g., notices that also function as warnings) and be considered active or passive [13]. The *active* communications interrupt users' activity so that they pay

attention while *passive* communications provide information to users without actively trying to get their attention.

When communications are delivered correctly to *human-receivers* without any impediments, they should generate appropriate security behaviours, as shown in Figure 2.1 [13]. The receivers, or the users, then process these security communications based on their personal variables, intentions, and capabilities before taking action.

According to Cranor [13], individual differences in users may affect the way they understand and apply security communications, as well as intentions and capabilities to perform appropriate behaviours. Therefore, the risk perception of warnings may depend on personal variables such as demographics and knowledge of the users like age, gender, culture, education, occupation, disabilities and prior experience [13]. Furthermore, users' intentions such as attitudes, beliefs and motivation may impact whether or not they heed to and comply with warnings, while users' capabilities such as cognitive and physical skills may be fundamental in executing appropriate actions [13].

We use the HITL framework to organize and guide the remainder of this background chapter. We focus primarily on the *Communication* and *Human Receiver* components of the framework since they are most relevant to our work.

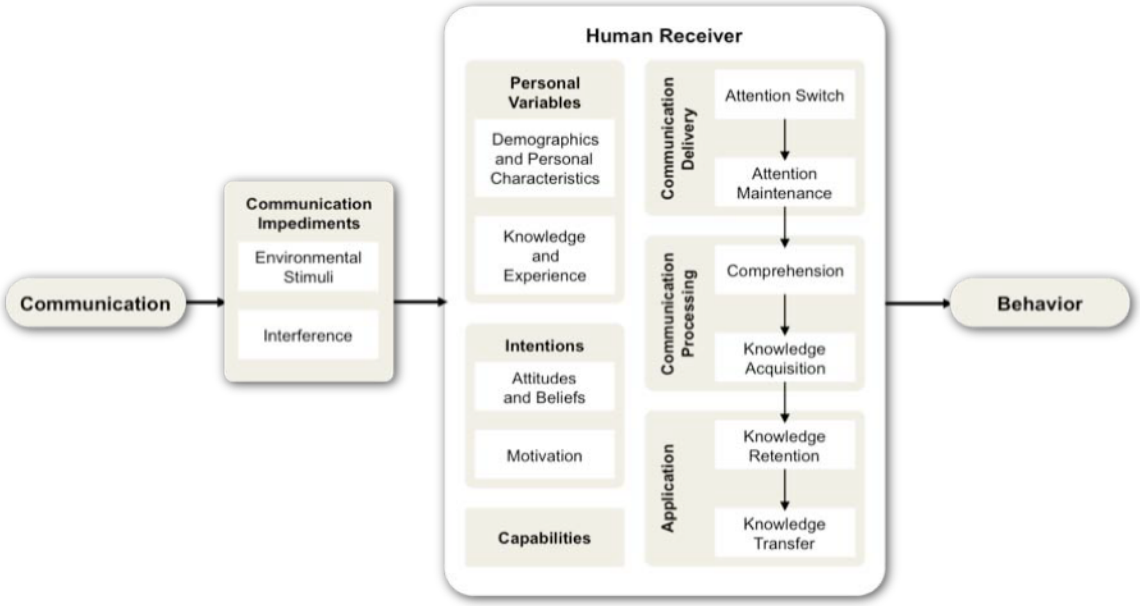


Figure 2.1: The human-in-the-loop security framework (HITL) by Cranor [13].

2.3 Communication

In cyberspace, users and their personal information, financial data, computers or mobile devices may be harmed by immediate or future threats [10]. Bravo-Lillo *et al.* [9] argue that computer security warnings should protect users and their computers, and that humans' psychological process in heeding, understanding and complying to cybersecurity warnings is similar to that of physical warnings. Humans respond better to physical or cyber warnings that are effective, communicate risk clearly, explain consequences of noncompliance, and provide instructions on how to comply [9, 63]. There are several things to consider when designing a system to communicate risk, such as the type of communication that will be the most effective, the severity of hazards the system has identified, and how much user action is required to avoid the hazard [13]. Our research focuses on security warning dialogs and notices.

2.3.1 Cyber Warnings

Bravo-Lillo *et al.* [9] categorized 29 security warnings from operating systems and applications into four warning types. We consider these as high-level categories, which include *information deletion or loss* (e.g., disk space warning), *information disclosure* (e.g., email-encryption warning), *execution of malicious code* (e.g., address book disclosure warning), and *trust in malicious third parties* (e.g., email attachment warning). For the purpose of this research, we identify three sub-categories of cyber warnings that are discussed by the participants and are more relevant to our study: exception messages, SSL certificates, and malware and phishing warnings. These warnings are issued by various operating systems, websites, browsers and antivirus software.

Exception Messages

Also known as "error messages", *exception messages* are observed when unexpected conditions occur or users perform unanticipated actions on computers and other devices [3]. They generally appear in secondary windows [3] such as dialog boxes or pop-ups. Figure 2.2 presents examples of exception messages. These warnings are

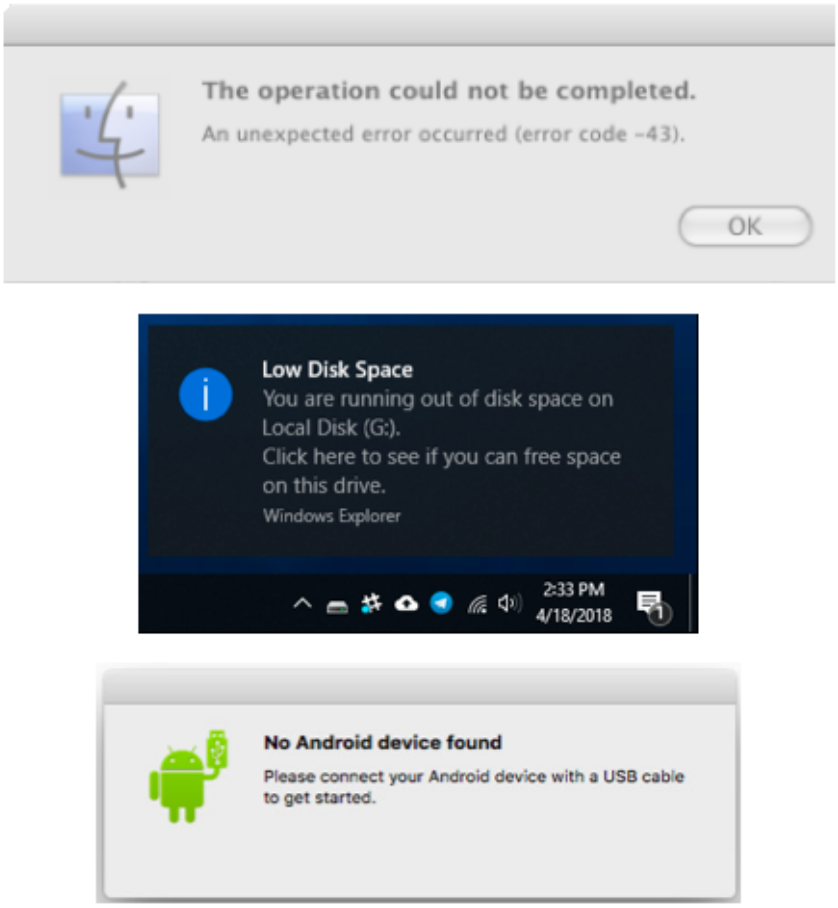


Figure 2.2: Examples of exception messages.

unrelated to cybersecurity but some users confuse these with security warnings, as observed in our study (Section 7.1.2).

SSL Certificate Warnings

The *Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols* are used to create secure links between websites and users' browsers [1, 17, 55]. These protocols warn users when encountering various server problems such as certificate expiration, or mismatched server addresses which could signal man-in-the-middle or Domain Name System (DNS) spoofing attacks [1, 55]. Figure 2.3 shows SSL certificates for Google Chrome. These warnings fall under *warning dialogs* and *notices* communication types, which inform users of the possible risk if they proceed to the

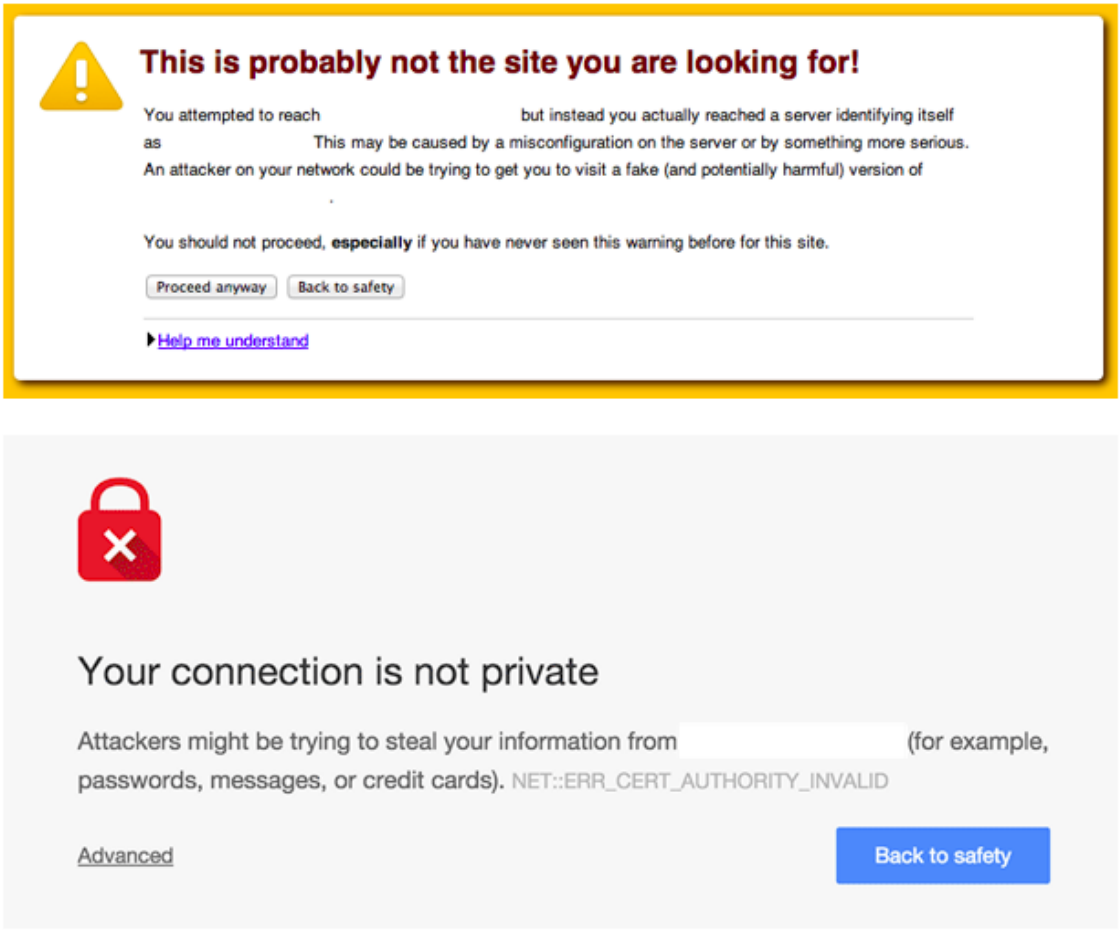


Figure 2.3: SSL certificates for Google Chrome.

website. Some of the security cues that these warnings use include colours and symbols (e.g., yellow yield sign with an exclamation mark inside, red lock with a warning X), and words that explain the threat source and the specific data that is at risk [57].

Malware and Phishing Warnings

Malware and phishing warnings notify users of potentially malicious and phishing websites [1, 2, 45]. Figure 2.4 presents malware and phishing warnings for Google Chrome. These warnings fall under *warning dialogs* and *notices* communication types. These warnings include colours and symbols (e.g., octagon with a red warning X on a red background), and words that explain the threat source and the specific data that is at risk. As browsers such as Google Chrome have had cases of false

positive for malware and phishing websites [51], they use bypassable warning messages that provide users the option to proceed [1, 2]. According to Akhawe and Felt [1], users ignore warnings when they do not read or understand them, assume that their devices can guard against the attacks via antivirus software, or the warnings are false positives. If the browsers are certain of a malware attack, they remove the bypassable option [1].

2.3.2 Design Parameters

There are various design parameters in cybersecurity warning messages. *Design parameters*, synonymous with design elements, refer to individual design components including colours, symbols and words [3]. In this thesis, we focus on signal colours, symbols and words, which are used to signal potential hazards to users encountering potentially harmful situations [3].

Signal Colours

Signal colours are one of the most common design parameters of physical and cyber warning messages [53]. Silic *et al.* [53] emphasize that we should consider which colour best communicates risk to users when designing warning messages because colour is a significant determinant of perceived risk and intentions to comply. Braun *et al.* [7] found that warning labels presented in colour were perceived to be more hazardous and readable than those presented in black-and-white.

Humans have the tendency to associate colours with everyday events, social norms and attributes. For example, in western cultures, the colours *pink* and *blue* are generally used to differentiate between girls and boys and *black* clothing is worn for mourning [25, 33]. Literature on affective colours show that younger children tend to love and are attracted to things that are bright and bold [24]. Boyatzis and Varghese [6] found that generally, children 5 to 6 years old associated bright and light colours (e.g., *red, yellow, orange, blue, pink*) with positive emotions (e.g., happiness, excitement, comfort) and dark colours (e.g., *black, grey, brown*) with negative emotions (e.g., sadness, anger). In a study examining college students' colour-emotion associations, Kaya and Epps [33] found that lighter and cooler hues (e.g., *green, blue,*

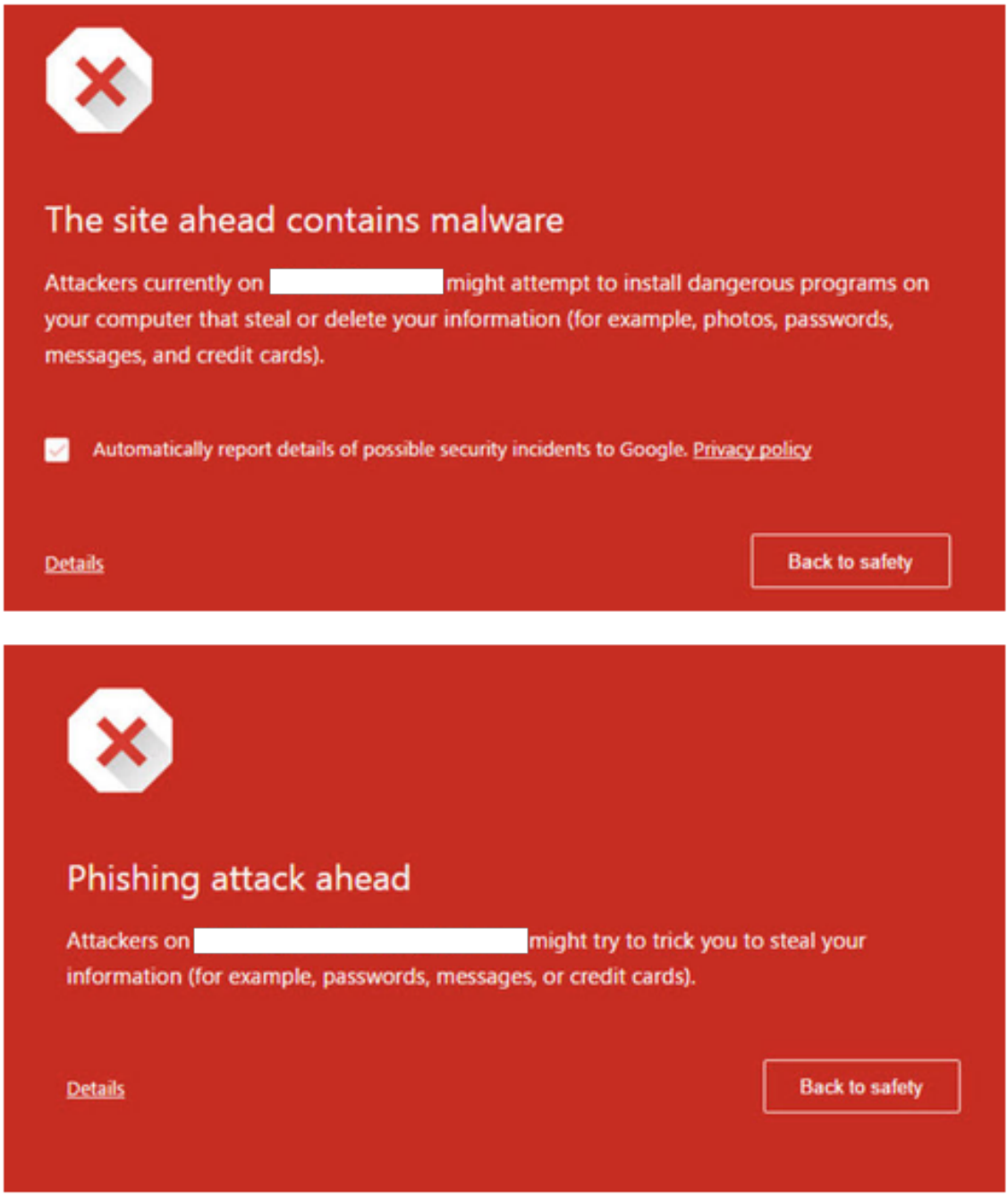


Figure 2.4: Malware and phishing warnings for Google Chrome.

white) were generally seen to be positive while darker shades (e.g., *black, grey*) elicited negative emotions. The perception of some colours 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) [33].

More familiar colours for warnings such as *red* are associated with a negative connotation in the context of cyberspace [53]. *Red* is often used as a symbol for high risk and is most preferred to grab human attention [25, 28, 36, 53]. Using differential and free-association techniques, Griffith and Leonard [25] determined that *red* had the strongest association with high levels of perceived hazard.

The general standards for physical warnings suggest that the colours *red*, *orange*, *yellow* and *blue* imply varying levels of risk, such as *severe*, *minor* and *none* respectively [25, 36]. Leonard [36] examined the perception of risk for colour words and signal words in the context of warning signs using a seven-point Likert scale from one having the lowest risk to seven having the highest. *Red*, *orange*, *black* and *yellow* were most highly rated by his adult participants. These results were consistent with previous studies with the exception of *orange* [25], which is commonly considered less serious than yellow. Colours *white*, *blue* and *green* were considered the least serious.

Similarly, Holtzschue [28] argues that some colours are important in communicating ideas. She mentions the Occupational Safety and Health Administration (OSHA) colours in the United States, where *yellow* represents *caution* while *orange* indicates *dangerous machinery or equipment*, *red* is used for *danger* and *stop*, and *green* suggests *safety*.

Colours have been discussed in the literature in relation to other design parameters and contextual associations. Griffith and Leonard [25] found that *red* was highly associated with the word *stop* and the *traffic stop sign*. They also associated *yellow* and *red* on *traffic lights* with *caution* and *warning*. *Black* was associated with signal words such as *fatal*, *deadly* and *poison*, and symbols such as *skull and crossbones*, a sign of death [25].

Signal Symbols

Fagan *et al.* [16] identified that participants perceived symbols and patterns as important parameters in attracting users' attention. Likewise, other research on warnings also mention that warnings with symbols are more likely to gain attention compared to those without [64]. Having *signal symbols* increases the salience and likelihood of warnings being noticed by users [3, 64].

In their study, Wogalter *et al.* [64] explained that symbols allow users to easily visually comprehend warnings, especially for groups of people who speak different languages or are illiterate such as children [64]. When designed correctly, symbols in warnings are able to reach and convey risk to the general population more effectively. Wogalter *et al.* [64] recommend that symbols and text should always be tested prior to implementation to ensure effectiveness.

Some symbols, such as *skull* and *exclamation point*, have been well studied in psychology in the context of consumer products and equipment [3]. On the other hand, little research has looked into the role and *arousal strength*[1] of signal symbols in the context of cybersecurity. Amer and Maris [3] addressed this research gap by examining arousal strength of signal symbols in information technology exception messages. Their results indicated that X had the highest perceived severity of hazard, followed by *!*, *?*, and *i*, with very little difference between *i* and *?*.

Exploring the impact of shapes on the perception of warning signs, Ma et al. [37] found that people have a stronger negative interpretation from the *upright triangle* than from the *circle*.

Signal Words

Words such as *danger*, *warning*, *caution* and *notice* are considered general standards for physical warnings, and are intended to elicit different levels of risk perception in users, such as *severe*, *minor* and *none* respectively [25]. In a study by Griffith and Leonard [25] on physical warnings, the word *danger* was considered to have the highest arousal strength. Leonard [36] found that the words *fatal*, *deadly*, *danger* and *warning* were considered very severe, and *notice*, *attention* and *caution* were less

[1] The severity/level of hazard communicated by the design parameters [3].

serious, which was consistent with his previous study [25].

Hellier *et al.* [26, 27] highlight the importance of mapping *signal words* with the level of risk implied by the hazardous situations that they indicate on physical warnings. Consequently, words that do not imply an explicit risk should not be used in severe warning messages. For instance, *careful* may be used in hazardous situations while *notice* should be used in non-risk situations [26].

Similar to their results for signal symbols, Amer and Maris' [3] study examining arousal strength of signal words with adults indicated that on exception messages, *critical* had the highest perceived severity of the hazard, followed by *urgent*, *warning*, *error*, and *notice*, with very little difference between *warning* and *urgent*.

2.3.3 Warning Design

Well-designed warning messages communicate risk effectively [9, 63] but must also attract attention at the appropriate time. To design warning dialogs that attract users' attention, Bravo-Lillo *et al.* [8, 11, 31] propose five attention attractors, four inhibitive and one non-inhibitive. Inhibitive attractors prevent users from proceeding until they interact with the warning or after a certain time has passed, while non-inhibitive attractors have an eye-catching stylistic change of text font and background [8, 11]. In order to get users' attention, their findings suggest that warning messages should force users to interact with the warning text.

Anderson *et al.* [4] found that polymorphic warnings were more effective in combating habituation than conventional warnings. To mitigate habituation effects, they propose a polymorphic warning design that has visual variations, such as messages that jiggle, change in size and colour, or show different symbols and words.

Findings by Akhawe and Felt [1] indicate that warning design can impact user behaviour; different types of warnings have different *clickthrough rates*[2]. The researchers point out that the differences in rates may be due to warning appearance and demographic differences among users. Thus, creating a systematic design of warning messages that incorporates user perceptions and experience may better persuade

[2]The proportion of users who clicked through a warning type by ignoring or making an informed decision to proceed [1].

users to carry out safe security practices.

Design Guidelines for Warnings

We present existing design guidelines for cybersecurity warnings.

An effective warning should not merely alert users of a potential or an existing threat, but should also clearly communicate risk, explain consequences of noncompliance, as well as instruct how to avoid or mitigate the risk [9, 63].

Bauer *et al.* [5] proposed a set of guidelines that may help designers and developers to create more effective cyber warnings. These guidelines were derived from current literature on usable security and warnings research from *Human Interface Guidelines* (HIG) for Windows, MacOS and Linux operating systems. The researchers suggest the following six guidelines:

1. *Describe the risk comprehensively*: The risk should be clearly identified and explained.

2. *Be concise and accurate*: The warning message should be simple, to the point, give correct information and not be overly technical.

3. *Offer meaningful options*: Warning dialogs should provide users with sufficient information so that they can decide between two or more meaningful options.

4. *Present relevant contextual information*: Warnings should present contextual information such as the consequences of noncompliance, so that users can make informed decision.

5. *Present relevant auditing information*: The user's device should maintain access logs and the warning should show whether the website or the application has been previously accessed.

6. *Follow a consistent layout*: Warnings should follow a common suggested layout based on the Human Interface Guidelines (HIG) [29, 50, 61] that they can be recognized easily by users. These elements include a single icon, primary text, secondary text, a question, a set of primary options, and a set of secondary options.

Wogalter *et al.* [64] also created a set of research-based guidelines for warnings. The researchers suggest that large, bold print, high contrast, colour, borders, symbols, and special effects like flashing lights and auditory sound increase the salience of a warning. Aligning with the cyber warning design guidelines mentioned above [5], Wogalter *et al.* [63,64] suggested that an effective warning should include four components: a signal word to attract attention, identification of the hazard, an explanation of consequences if exposed to the hazard, and instructions for avoiding the hazard.

Design Guidelines for Children

While studies have been conducted to examine hazard matching of design parameters for cybersecurity warning messages [3, 16, 25–27, 36, 64], there is a limited number of empirical studies to establish recommendations for children.

Micheti *et al.* [43] identified 14 guidelines for writing privacy policies that children and teenagers can easily comprehend. These guidelines include textual elements on comprehension, structure of the text and the overall design of the privacy policies. Although these guidelines specifically relate to privacy policies, several guidelines appear relevant for warnings too:

1. *Guideline 1*: Choose the simplest words possible.
2. *Guideline 2*: Avoid double negatives.
3. *Guideline 3*: Use language that makes clear who is doing what to whom.
4. *Guideline 4*: Keep sentences simple and paragraphs short.
5. *Guideline 5*: Put the main idea of the sentence at the beginning.
6. *Guideline 7*: Arrange information in a logical order.
7. *Guideline 8*: Group related information together and eliminate redundancies.
8. *Guideline 9*: Provide informative headings.
9. *Guideline 13*: Leave enough white space.
10. *Guideline 14*: Use, but do not overuse, emphasis techniques.

2.4 Human Receiver

The *human receiver* is the user who receives the security communication and whose actions affect system security [13]. This section will focus on users' personal variables and intentions, and communication delivery information processing.

2.4.1 Personal Variables and Intentions

Personal factors such as demographic variables (e.g., age, gender, cultural background, education, occupation, and disabilities), knowledge, familiarity, experience and training with warnings or tasks, and individual differences in their intentions such as attitudes and beliefs contribute to *warning effectiveness*[3] and how users are likely to behave in security-critical situations [13, 64]. We summarize the literature addressing children and adults' risk perception in the context of cybersecurity.

Adults and Online Risk Perception

The majority of the literature on cybersecurity warnings and user perception focus on adult users. Research on adults and perceived online risk often discuss user perception for two user groups: expert and novice users [9, 13].

Aesthetics play a huge role in the perceived credibility of interfaces [49] and how users behave [2]. Sometimes, users decide if a site is credible or not based on look-and-feel alone [49]. Bravo-Lillo *et al.* [9] found that novice users consider the security warning's look-and-feel soon after they encounter dialog pop-ups to determine how suspicious or credible they are. The website's reputation and credibility highly affect how users react to warning scenarios [2]. Participants mentioned that they would ignore the warning against high-reputation and credible websites while they would heed a warning against low reputation and less credible websites because they did not trust these sites [2].

Bravo-Lillo *et al.* [9] found that expert and novice adult users observed different cues and made different conclusions about the security warning risks. While experts assessed how safe their actions are *a priori* or from deductive reasoning, novice

[3] How effectively the warning communicates risk [1].

users generally assessed risk after engaging in their actions [9]. Expert adult users performed security actions such as researching risks that they faced online through public expert forums, regularly updating their software like antivirus programs and security plug-ins, and using safe and legitimate URLs compared to novices [9].

Expert users with training and experience related to cybersecurity may be more likely to understand complicated instructions, overthink and second-guess security warnings, or perceive less risk than novice users [9, 13]. For example, experts ignore warnings when they understand them because they believe they are unimportant, while novice users cannot assess whether they are at risk because they do not understand the attack [9].

Children and Online Risk Perception

Research has shown that online security and privacy warnings are frequently ignored or misinterpreted by even experienced adult users [1,9]. Children may be particularly vulnerable because they are not always aware of the risks associated with online threats [67].

According to literature on children's developmental stages, children not only differ from adults but they behave and perceive differently at varying stages of development [49]. In the *sensorimotor stage (birth to 2 years)*, children begin to understand the world from the information they receive through their senses and movement. In the *pre-operational stage (2 to 7 years)*, children develop an understanding that objects can be represented through words and symbols. In the *concrete operational stage (7 to 11 years)*, children are able to see through others' viewpoints, classify things, and understand the idea of reversibility and conservation. In the *formal operational stage (11+ years)*, children can think abstractly and logically, and deal with hypothetical situations.

Children in the late concrete operational stage and early formal operational stage are the main user groups in our research. Children who are 10 years old begin to use social networking platforms, watch online videos, visit virtual worlds, and play online games [41]. Children 11 to 12 years old begin to actively communicate online, watch and download music, movies and TV shows online, and may be vulnerable in

giving out personal information to online marketers [40]. At this age, children should be developmentally able to start recognizing warning messages, consider the possible consequences of their actions, and make logical decisions if information is presented to them in an age-appropriate manner.

Compared to adults, however, Zhang-Kennedy *et al.* [67] suggest that children's perceptions of cybersecurity are less developed. While children believed that their privacy was important, only half actually understood what it meant to stay private online. Interestingly, children between the ages of 7 to 11 years old perceived internal privacy threats from siblings and parents to be more serious than external threats from friends, strangers or online media [67].

Davidson and Martellozzo [14] identified that although young people in the UK aged 12 to 18 years old seemed knowledgeable about safety and risks online, they did not perform preventative behaviours. Furthermore, these researchers found a lack of awareness among children for whether something is considered personal information. They conducted their study in both the UK and in Bahrain. They also discovered that gendered cultural issues highly affected children's online behaviours. Twenty percent of children in the UK had "threatening" experience online from strangers or acquaintances such as cyberbullying, while 36% of children in Bahrain had been made to feel "uncomfortable" online and more girls (43 %) experienced these situations than boys (32 %) [14]. Another study conducted in Greece reported a significant increase in experiences of online cyberbullying among high school students [19]. These demographic variables and prior experiences contribute to children's online risk perception.

Risk Communication through Metaphors

How warning messages are perceived may be greatly influenced by how the risks associated with these warnings are communicated to end-users. Current literature suggests that *risk communication* is poor in the field of computer security [12].

To improve risk communication in cybersecurity, Camp [12] suggests five security *metaphors*[4]: physical, medical, criminal, warfare, and market models. *Physical*

[4]Camp [12] calls these mental models by using metaphors to explain a particular element of a system based on an expert understanding. For the purposes of our research, we will refer to them simply as metaphors.

security model can motivate users to secure their computers from "intruders" by communicating actions such as locking down their system, while using the *medical model* allows users to make connections between malicious code and infectious diseases, thus emphasizing the importance of identifying and responding to a virus [12]. The *criminal model* suggests that users should protect themselves and their computers from cyber-"criminals" such as hackers by tracking and prosecution. The *warfare model* communicates the idea of a "determined implacable enemy" and to think of "firewalls", tight constraints on the network and limited connectivity, as defense technologies, while the *market model* can be used to identify "costs" and "externalities" due to security failures.

The medical metaphor shows potential in communicating cybersecurity risks to users because the model acknowledges that everyone is at risk and emphasizes the importance of autonomy and shared responsibilities for community health [12]. Therefore, Camp [12] argues that the *medical model* may be the most effective risk communication method to use in cybersecurity context. These mental models are in no way perfect [12]; the metaphors they use may not apply to every security situations nor be the most effective in mitigating risks. Accordingly, it is highly recommended that these models be further tested via user studies [9, 12].

Hazard Matching

Hazard matching refers to successfully mapping risk to warnings. In the cybersecurity context, the severity implied by the warning message should match the level of hazard perceived by the user [3, 27].

According to Hellier *et al.* [27], warnings implying various levels of risk can be used in situations that range from minor to highly hazardous circumstances. Matching the perceived risk with the actual level of hazard implied by the warnings may help to effectively communicate and distinguish highly hazardous situations from the less dire, which in turn may improve the informativeness of warnings. Warnings should communicate both the presence of threat and its severity [3, 27].

To achieve hazard matching, we must establish a systematic relationship between warning design parameters and perceptions of hazard [27]. Some examples of design

parameters include variations of signal colours, words, symbols and message sizes [3, 27]. There are several research methods that can be used to map risk to design parameters. In their experimental study, Hellier *et al.* [27] asked participants to rate arousal strength using techniques such as Likert ratings, cross-modality matching and free modulus magnitude estimation. From triangulation, the researchers confirmed that arousal strength scales of signal words are robust, and thus, signal words can be used to achieve hazard matching. Similarly, Amer and Maris [3] used a ten-point Likert scale for participants to indicate the perceived degree of severity of the exception message. When the arousal strength is established, warning messages can be better matched to situations with varying levels of hazard [3, 27].

Each person is unique, and therefore, may perceive risk differently. In her behavioural study of consumer product warning labels, Otsubo [48] found that perceived differences in the level of "hazard" or "danger" between products influenced people to heed, read and comply with warnings, which in turn affected warning effectiveness.

2.4.2 Communication Delivery

Communication delivery is the first step in information processing that includes attention switch, users taking notice of the communication, and attention maintenance, users maintaining their attention to the communication long enough to process it [13].

Habituation Effect

A major inhibitor of the effectiveness of security warnings is the *habituation effect* [3, 4, 31, 32, 58]. Experimental studies on the effect of habituation support this claim [1, 4, 58].

Habituation refers to the decline of user attention and eventual desensitization to a stimulus because users are frequently exposed [4, 31, 32]. After repeated exposure to warnings, people are less likely to pay attention and attend to the message, which leads to a decrease in compliance [3]. Furthermore, when users cannot immediately see or experience the consequences of non-compliant behaviours, they may begin to respond habitually to warnings despite changes in the context or the information in the message [31]. For instance, if warning messages for two different hazardous

situations look similar, users may develop automated response and replicate their reaction across both situations, which may lead to noncompliance or inappropriate response [3].

Results from the study by Amer and Maris [3] confirm that habituation decreases the effectiveness of exception messages. Some ways to mitigate the ramifications of desensitization to warnings are altering the parameters of the messages such as using signal words and icons that have varying levels of arousal strength depending on the context [3], and applying polymorphic variations [4, 58]. For example, a program could monitor users' response time and attention to warnings that has been displayed multiple times, and if the program detects a decline in attention, it could display a differently designed message [3]. More studies need to be conducted to further test these results.

Theory of Warning Fatigue

Similar to the habituation effect, *warning or alert fatigue* occurs when users become desensitized to the stimulus [1, 38]. As users continue to receive more and more warnings, their attention may decrease and reaction time may increase, eventually resulting in failure to comply or respond appropriately. According to Masters [38], warning fatigue is the threshold at which recognizing the urgent warnings from others becomes difficult for end-users. Like *crying wolf* [38], a phenomenon that results from being over-warned by false alarms, we have become immune to warning messages that would otherwise be recognized as real danger.

In their large-scale field study on browser security warning effectiveness, Akhawe and Felt [1] observed that participant behaviours were consistent with the theory of warning fatigue. In their study, the clickthrough responses for common error messages were faster than for less common errors due to the effect of warning fatigue. As a result, they advise for security practitioners and designers to consider limiting the number of warnings shown to users [1]. The researchers suggest that future studies should focus on the effect of user demographics on browser warning effectiveness.

2.5 Research Gap

Warning messages should only be used as the last lines of defense when it is not possible to eliminate or design a system that fully shields against a hazard [1, 4, 9, 13, 55, 63]. When designing such system is not feasible, we need to rely on warning messages that are effective. Current literature indicates that warning messages can be successful in advocating for safe security practices in users if designed properly [1]. However, it is critical for security practitioners to understand their primary target users and the severity of hazard perceived by the users [1]. Currently, there is a lack of research exploring children and their perception of warning messages.

To address this research gap, our thesis will first aim to understand how children and adults perceive the severity of hazard associated with three warning design parameters: signal colours, symbols, and words. The empirical findings from this research will establish children's perceptions of security warnings in comparison with adult users, and help identify warning message design features that may communicate more effectively to children.

Chapter 3

Methodology

Effective security warnings should be tailored for all types of users, especially those who may be more vulnerable. Compared to adult users, children may not always be aware of the risks associated with cyberthreats [67].

There is a lack of research on children and their risk perceptions of cybersecurity warning messages to establish design recommendations. To design more effective warning messages for children, we conduct user studies to see how they perceive the severity of hazard associated with three basic warning design parameters: signal words, colours and symbols. To our knowledge, no in-depth empirical study has been conducted to explore children's perception of these parameters independently.

To fully understand children's perception and comprehension of security warnings, we also observe adults' perspective because current cybersecurity warnings are typically designed for adult users [22, 42] and their data can serve as a baseline. The results from both user studies will be compared and contrasted to establish similarities and differences between children and adults, and to provide recommendations to design better warnings for children.

The main research question in this thesis was as follows: *"How do children and adults compare in their perceptions and understanding of signal colours, symbols, and words in the context of cybersecurity warning messages?"*

This question was explored through three sub-research questions: RQ1) *Children's perception of severity of hazard: How do children comprehend and perceive the severity of hazards associated with warning design parameters (signal colours, symbols, and words)?* RQ2) *Adults' perception of severity of hazard: How do adults comprehend and perceive the severity of hazards associated with warning design parameters (signal colours, symbols, and words)?* RQ3) *Comparison: How do the two groups compare?*

3.1 Hazard Matching

Our research methodology was inspired by the works of Amer and Maris [3], Bravo-Lillo *et al.* [9], Hellier *et al.* [27] and Wogalter *et al.* [64].

Hazard matching is when the severity of hazard communicated by the warning matches the user's perceived severity [3, 27]. In order to achieve this, a systematic relationship between variations in warning design parameters and variations in user's perceived levels of hazard should be established [27]. The first step is to scale the perceived arousal strength of each design parameter (quantifiers of risk) by asking users to rate their severity [3, 26, 27, 64].

To collect users' subjective measures, we used categorization followed by ranking methods to scale the perceived arousal strength of items within each parameter. Since this method may be susceptible to response bias [27], we followed the activity with an interview to clarify the dimensions that were important to each participant as suggested by Wogalter *et al.* [64]. Sorting and ranking were chosen because they seemed to be the simplest task for children, compared to other techniques such as Likert rating and free modulus magnitude estimation [27].

3.2 Ethics and Recruitment

Our research methodology was reviewed and cleared by the Carleton University Research Ethics Board-B (CUREB-B). This research was divided into two studies; the first involved 22 child participants and the second had 22 adult participants. The participants were recruited through social media, recruitment posters, and snowballing methods (Appendix C). The study was advertised on the Carleton Research Participants Facebook group and other social media accounts such as LinkedIn and Twitter. Recruitment posters were placed on billboards at Carleton University in accordance with Carleton's posting policy and around public areas within Ottawa community with permission, such as local public libraries. Participants who emailed the researchers were invited to take part in the study.

Eligible participants included children between the ages of 10 to 12 years old and adults over 18 years old, who were comfortable speaking and reading in English.

The research activities and interviews took place in the Carleton's Human Oriented Research in Usable Security (CHORUS) laboratory on campus or in a mutually agreed upon public space that was familiar and comfortable for the participants. Public venues included the private meeting rooms in the public libraries where an adequate amount of privacy and confidentiality were provided. We obtained written consent from the parent/legal guardians and adult participants, and verbal informed assent from the child participants. In appreciation for their time, the participants received 20 dollars cash and the cost of parking if the session took place on the Carleton campus.

3.3 Materials

For the card sorting and ranking activities, we used a total of 60 laminated standard size business cards that each had a different signal word, colour or symbol (Figure 3.1). The list and template of all the cards are included in Appendix B. The cards were created on Adobe Illustrator and the CMYK colour model was used for printing. To determine the specific signal characteristics that would be used, we began with a literature review and web searches of existing cybersecurity warning messages. We collected 80 examples of warning messages from peer-reviewed articles, books, 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 such as Chrome, Safari, Internet Explorer and Firefox, social networking services such as Facebook, LinkedIn, Twitter and Instagram, and sample fake warning messages. From the examples collected, we then extracted the most commonly repeated signal words, colours and symbols, including some of which may be used outside of the cybersecurity context. For example, we extracted *fire* and *skull and crossbones* symbols even though they were generally found on consumer and WHMIS products rather than cyberwarnings.

3.3.1 Word Selection

From our findings and the literature [25–27,36], we gathered 36 common signal words. We ran a pilot test using a survey hosted on Qualtrics that asked 6 cybersecurity and

Figure 3.1: Example of cards used for card sorting and ranking activities.

design researchers to openly categorize the words with similar meanings into 20 self-selected, user-defined groups and to rank them in the order of most relevant security word to the least relevant in each group. We tabulated the results and selected the highest ranked word in each of the 20 categories. These 20 words were printed on individual cards for use in our main study (Figure 3.2).

3.3.2 Colour Selection

We discovered that there were limited set of colours that are typically used in warning messages. To be consistent in number with signal words and symbols, 20 colours were chosen from a palette of colours that were considered individually distinctive. These included the colours commonly found on warning messages [25, 36]. Each colour was printed on a card as a large coloured circle with its name below it so that the participants could easily name them (Figure 3.3).

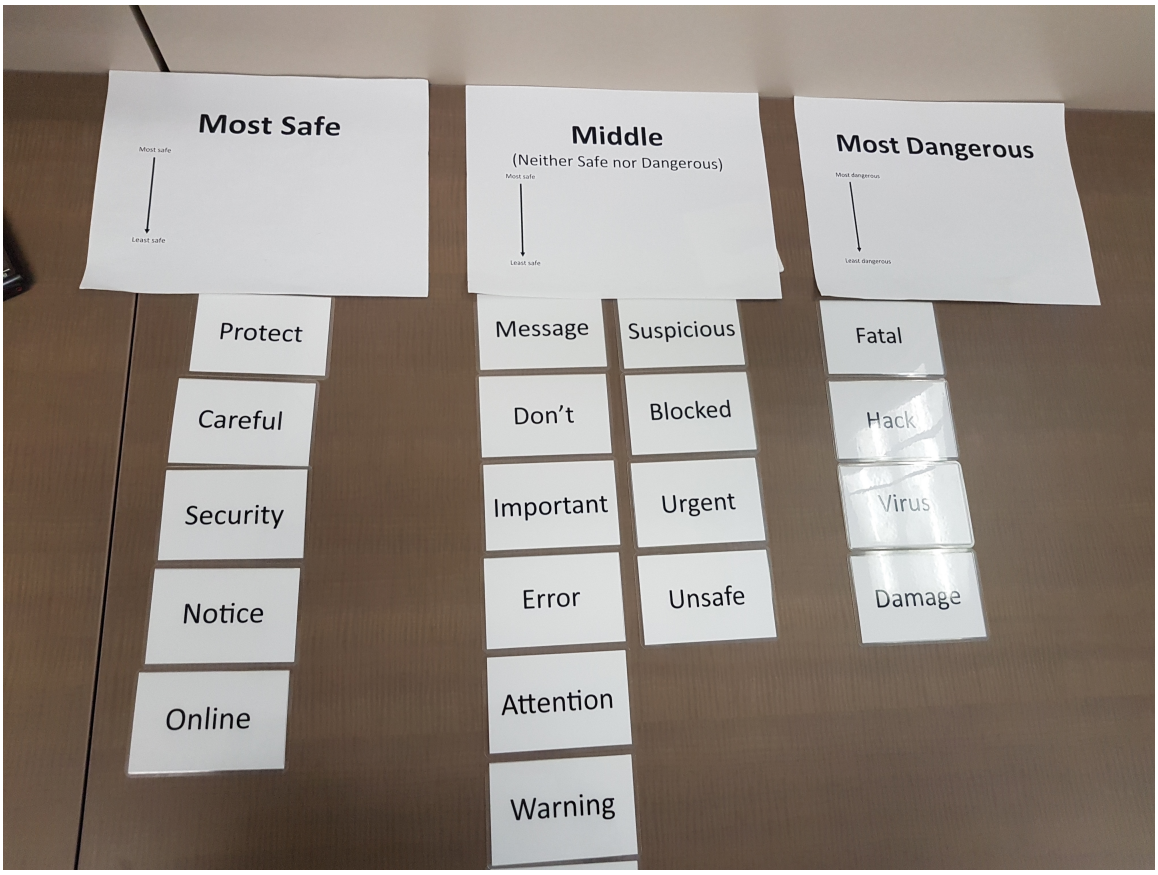


Figure 3.2: An example of the sorted signal word cards during a user study session.

3.3.3 Symbol Selection

The 20 signal symbols chosen were simple, printed in black and white, and found in general warning messages within and out of context of cybersecurity warnings [3,20,21,25,36,46]. These symbols were also printed on individual cards (Figure 3.4).

We also 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".

Figure 3.3: An example of the sorted signal colour cards during a user study session.

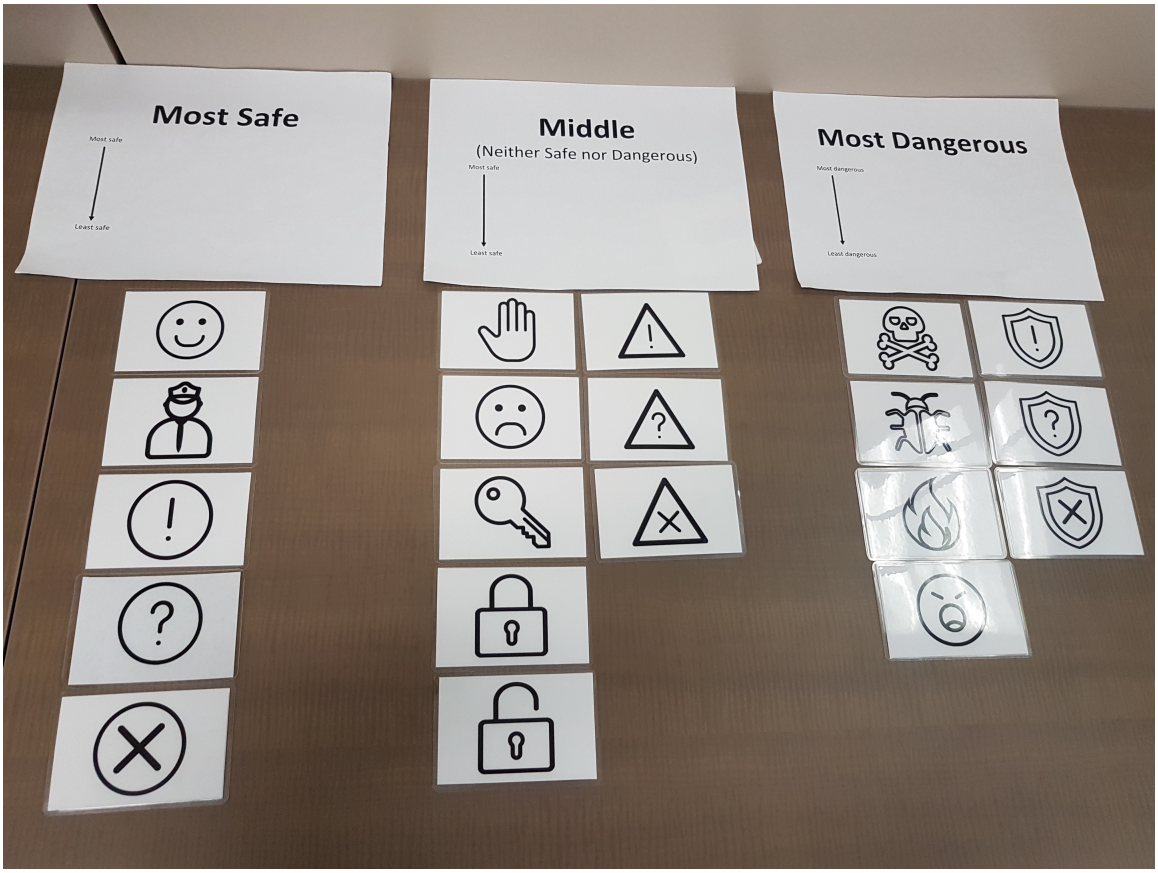


Figure 3.4: An example of the sorted signal symbol cards during a user study session.

3.4 Protocol

After participants had provided their informed consent and assent, the study sessions included three segments: 1) *Pre-test interview* 2) *Card sorting and ranking activities* 3) *Post-test interview*.

Each study session took approximately 1 hour in total and was conducted as follows.

3.4.1 Consent

In Study 1, child participants were greeted and their parent/legal guardian was asked to read and sign the consent form for the child's participation. Assent (verbal informed consent) was obtained from the child if they agreed to participate. In Study 2, adult participants were greeted and asked to read and sign the consent form for their participation.

They were reminded that the session would be audio-recorded. They were also reminded that photographs would be taken of the final card placement once sorted and ranked. Participants were not photographed. The study began when consent was given. The researcher explained the purpose of the study and provided an overview of the card sorting and ranking activities. The consent forms and assent script are included in Appendix D.

3.5 Study Steps

1. **Pre-test interview**: The participant completed a short pre-test interview which collected their demographic and online and electronic device usage data. These questions were completed verbally. The researcher audio-recorded the participant's responses and took notes. These recordings were later transcribed. Some of the demographic information gathered about our participants was inspired by other studies on warning messages [3, 16, 42]. For demographic information for child participants, we asked for age, school grade and sex. For adult participants, we asked for age, highest level of education completed or currently

enrolled, current employment status, and the current program of study or occupation. For online and electronic device usage information, we asked both user groups for the day(s) per week and hour(s) per day being online, prevalence of being online during the week and weekend, and the types of electronic devices used to go online.

2. **Card Sorting and Ranking Activities**: The participant completed the card sorting and ranking activities. The cards were divided into three decks of signal words, colours and symbols. The cards were shuffled and the decks were presented to the participants one set a time using a Latin Square design to mitigate order bias. Table 3.1 depicts the number of participants that completed the activity in each randomized order of decks. After each deck was sorted on the table into the three categories, participants 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 placement of the cards. They could re-sort and re-categorize the cards if they changed their minds. This information allowed us to gain insight into their for each warning characteristic. If their explanations were unclear or ambiguous, we probed participants with open-ended questions regarding individual signal words, colours and symbols such as, "Could you explain your reasoning behind why you placed that card in this category?" The researcher took photos of the final results of the participant's sorting and ranking activities.

3. **Post-test Interview**: The participant verbally completed a post-test semi-structured interview regarding the perceived difficulty of categorizing the signal words, colours and symbols, and their previous experience with cybersecurity warning messages. We asked the participant to tell a story about coming across a warning message, and asked them to explain what they would expect to see on a dangerous warning. The participant was encouraged to expand on their answers to give more context.

Deck Order	Number of Participants
WCS	4
WSC	4
CSW	4
CWS	4
SWC	3
SCW	3
Total	**22**

Table 3.1: Number of participants that completed the card sorting and ranking activities in each order of 3 decks of cards based on a Latin square design. W = Word, C = Colour, S = Symbol.

3.6 Data Collection

All questionnaires and the interview script used during the sessions are listed in Appendix E. We asked the questions verbally and recorded responses and took notes on Microsoft OneNote. Each session was audio-recorded and transcribed by the primary researcher and an undergraduate research assistant. We took photos of the final card arrangements and transcribed those to Excel spreadsheets.

3.7 Data Analysis

We draw from more than 44 hours of transcribed audio-recordings with 22 child participants 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.

3.7.1 Quantitative Approaches

The final placement of the cards for both studies were recorded by the researcher based on the photos taken at the end of each activity (3.2). They were analyzed on 6 separate sheets on Microsoft Excel, organized individually by signal colours, symbols and words, and the participant groups (Appendix G). We calculated the median rank of each signal item (e.g., red) and ordered them based on the smallest median to the largest for each design parameter (e.g., colour). We chose the median values to rank

the items because on a set of ordinal data, median is more representative than the mean. A high standard variation and presence of outliers may be observed with the mean values. The results from child and adult participants were compared.

3.7.2 Qualitative Approaches

We applied content analysis methodology [15, 34, 65] to analyze the qualitative data. In the preparation stage, 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 a process called abstraction.

Through this methodology, we identified conceptual thematic mind maps for signal words, colours and symbols (Appendix F). Thematic mind map is a tool to visualize and organize themes and sub-themes in qualitative analysis [59]. Using these mind maps, we identified 7 major coding themes describing users' perceptions (Appendix F):

1. *Level of danger*: An assessment of how safe or dangerous a *signal item*[1] is perceived by the participant (e.g., *safe* or *dangerous)*

2. *Association with same parameters*: When the participant specifically mentions associations (similarities or differences) with other items in the same deck of cards (e.g., *red* and *maroon*).

3. *Association with other parameters*: When the participant specifically mentions associations (similarities or differences) with items in a different deck (e.g., *black* and *skull and crossbones*).

4. *Contextual associations*: When the participant specifically mentions associations relating to other contexts (e.g., technology, food).

[1]For the purpose of this research, any singular signal colour, word or symbol will be referred to as a signal item.

5. *Subjective perception*: The subjective attitudes and perceptions in relation to a signal item (e.g., attention grabbing).

6. *Ambiguous*: When the participant reports a signal item to be unclear or neutral, or when they "do not know" where to place the card.

7. *From previous experience*: When the participant mentions a previous experience with the signal item.

Using NVivo qualitative data analysis software [30], the primary researcher exhaustively coded all card categorization and ranking response transcripts and conducted analysis to further refine the themes. An undergraduate research assistant independently performed additional analysis on NVivo for 20 percent 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 there were discrepancies in the analysis, the researchers reviewed the coding and reached a common understanding or retained the differences in the analysis by using codes applied by both researchers. For example, if one researcher applied code 1 and the other applied code 2 to an excerpt, both codes were counted in the groups of categories and sub-categories during the analysis process. If new themes emerged or common themes were discovered by the secondary researcher, both researchers reviewed and decided to either include or disregard the new theme in the analysis. These new themes were added to the codesheet and applied to all transcripts.

A Cohen's Kappa (k) test showed strong agreement between the two researchers' analysis of the qualitative themes from card categorization and ranking with children ($k = 0.88$, 95% CI: 0.56 to 1.00, $p < 0.005$), and with adults ($k = 0.92$, 95% CI: 0.63 to 1.00, $p < 0.005$).

For post-test interview transcripts, only the primary researcher performed inductive content analysis. As the analysis for the post-test was completed by one researcher, there may be some bias towards single perspective. We recommend that future analysis be completed by multiple coders to assess intercoder reliability.

Chapter 4

User Study with Children

We aim to understand how children perceive the severity of hazards communicated by various parameters of cybersecurity warning messages such as signal colours, symbols and words through empirical data collected from a user study. The findings from this study will inform us of how children determine how children interpret these cues, and their expectations for effective warnings. The results could then be used in design to align the perceived severity of a hazard in warning with the level of hazard faced by the user [26].

4.1 Participants

We recruited 22 child participants for the first study. This number is appropriate based on Fugard and Potts' [23] sample size recommendation for thematic and content analysis used to identify qualitatively different patterns across a multiple-participant dataset. We set the lowest prevalence for a theme at 30% (0.3) with the likelihood of 50% that people who could say something relevant to a theme would actually say it. This gives an adjusted prevalence of 15% (0.3 x 0.5 = 0.15). Using Fugard and Potts' [23] tool, the recommended sample size was 19 for 15% adjusted prevalence, 2 instances were required for the theme to be recognized, and 80% power was needed to find the least common theme. We used these numbers as a guide and included 3 more participants to have a sample size large enough that would likely to reveal at least once any belief held by 10% or more of the population [44].

Table 4.1 details the participants' demographics. The 22 child participants were between the ages of ten to twelve, with the age average of 11 years (SD=0.65) and the school grade average of 6 (SD=0.64). There were 15 males and 7 females. They

ID	Sex	Age	School grade	Days/week	Hours/day
C01	Male	11	6	6	-
C02	Female	11	6	4	-
C03	Female	10	5	1	-
C04	Male	12	7	2	-
C05	Female	10	5	7	3
C06	Male	11	6	7	1
C07	Male	11	6	4	1
C08	Male	11	6	7	1
C09	Female	11	6	5	4
C10	Female	11	6	7	5
C11	Male	10	5	7	1
C12	Male	12	7	4	-
C13	Male	11	6	7	2
C14	Male	10	5	7	7
C15	Male	11	6	2	1
C16	Male	11	6	5	2
C17	Male	11	6	7	2
C18	Male	11	6	3	1
C19	Male	12	7	7	4
C20	Female	12	6	7	1
C21	Female	10	5	3	3
C22	Male	11	5	2	1

Table 4.1: Child participant demographics.

were online an average of 5 (SD=2.05) days per week, for an average of 2 hours and 28 minutes per day (missing 5 data points). Children used a variety of devices to go online and the most popular devices used were iPad (n=21) and laptop computer (n=21), followed by desktop (n=15), iPhone (n=14), Android phone (n=14), other tablets (n=12), gaming consoles (n=7) and Blackberry (n=1). All children (n=22) had experience in using more than one device to go online.

The children engaged in various types of online activities summarized in Figure 4.1. They went online primarily for entertainment purposes, through games (e.g., Roblox, Minecraft) and media (e.g., YouTube, Netflix). Half of participants used a *search engine* such as Google and *social networking services* (SNS) such as Instagram, Snapchat, Twitter and Facebook.

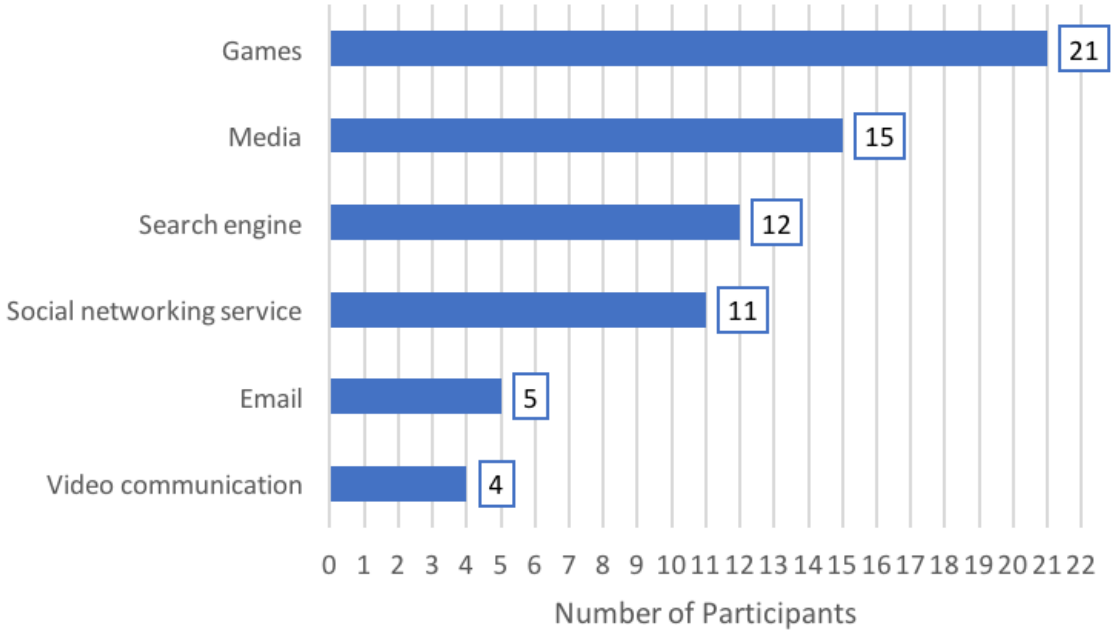


Figure 4.1: Children's online activities.

4.2 Results

The results from this study will summarize children's card categorization and ranking, qualitative findings, and post-test semi-structured interview.

4.2.1 Card Categorization

Participants were asked to categorize each set of cards into three categories of perceived severity of hazard (most safe, middle, and most dangerous). We first present the results of colour categorization.

Categorization of Signal Colours

Figure 4.2 represents the categorization of colours into three severity categories. The Y axis represents the colours ordered by largest value in most dangerous category, followed by middle and the least dangerous. The X axis represents the number of participants that placed each colour in each category.

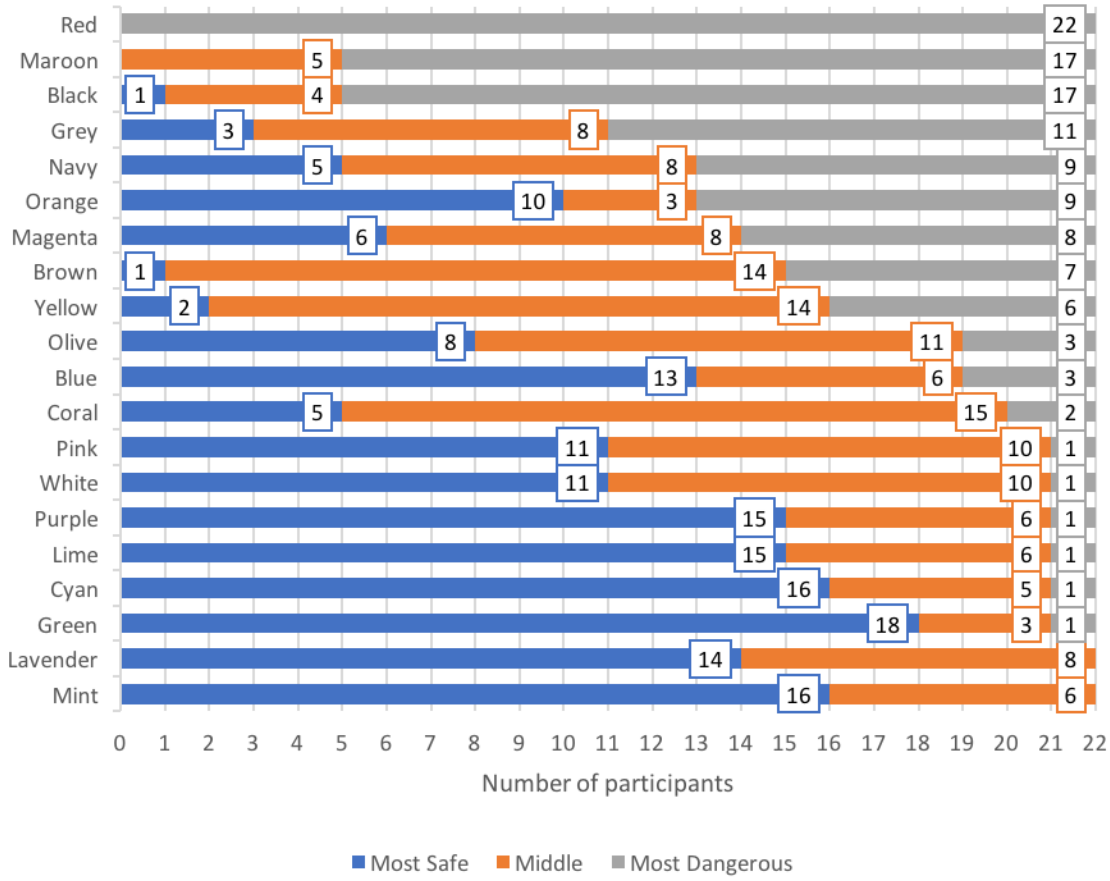


Figure 4.2: Number of children placing colours in each severity category.

Following cultural norms [25, 28, 36], *green* was considered the most safe colour (n=18, 82%) while *red* was considered the most dangerous (n=22, 100%). Generally, lighter and cooler shades were considered safer while darker shades were more dangerous.

Based on participant feedback, children commonly felt that it was more difficult to categorize the colours than the other two warning parameters (n=16, 73%). Some of the reasoning behind the difficulty in categorizing the colours include: uncommon colours for warning messages, lack of experience seeing some of the colours online and lack of context or explanation when using only colours.

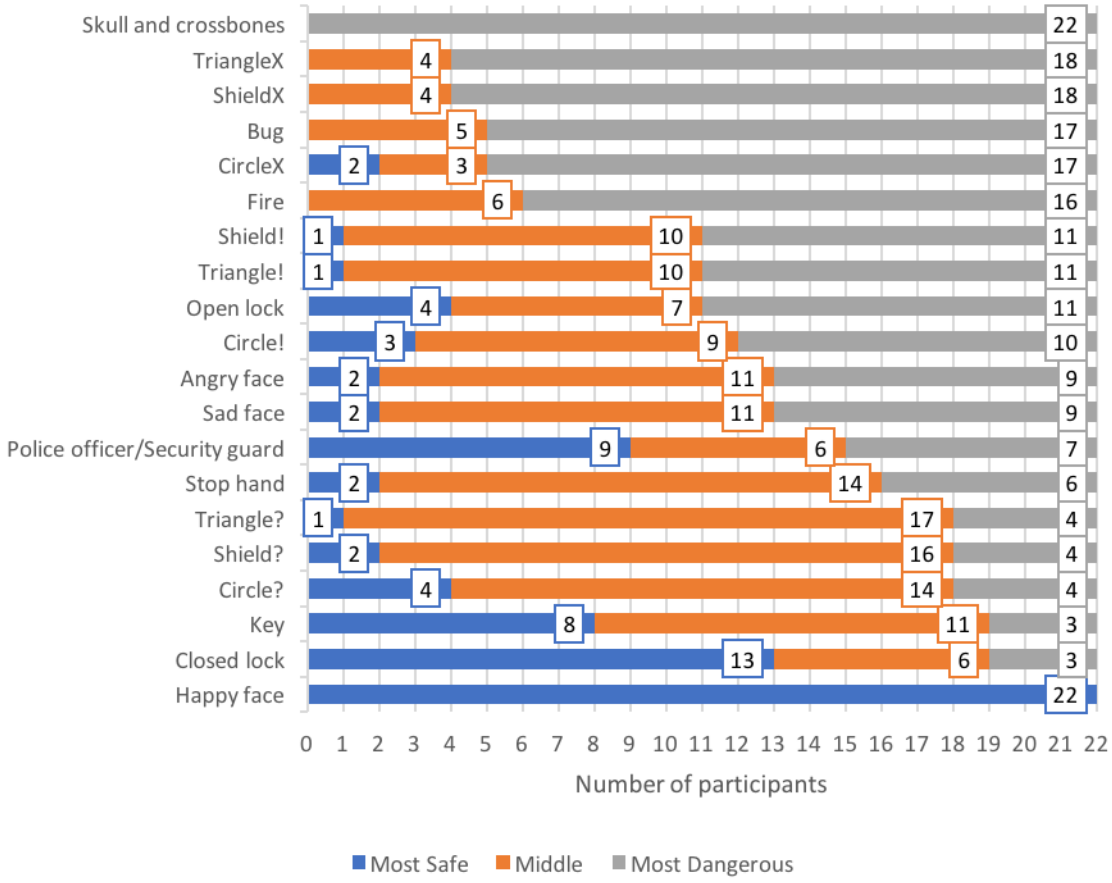


Figure 4.3: Number of children placing symbols in each severity category.

Categorization of Signal Symbols

Figure 4.3 summarizes the categorization responses for symbols. Uniformly, all participants believed that *happy face* was considered most safe (n=22, 100%) and *skull and crossbones* was most dangerous (n=22, 100%). Looking at the figure, we see that participants were generally unlikely to categorize symbols as safe. Interestingly, symbols that are common in security warning messages (i.e., *closed lock*, *police officer/security guard*, *key* and *open lock*) have high categorization variability with participants having different opinions on how to interpret the symbols. Symbols frequently observed on hazardous material labels (i.e., *skull and crossbones* and *fire*) were likely to be considered dangerous.

Although the least difficult to categorize out of the three warning parameters,

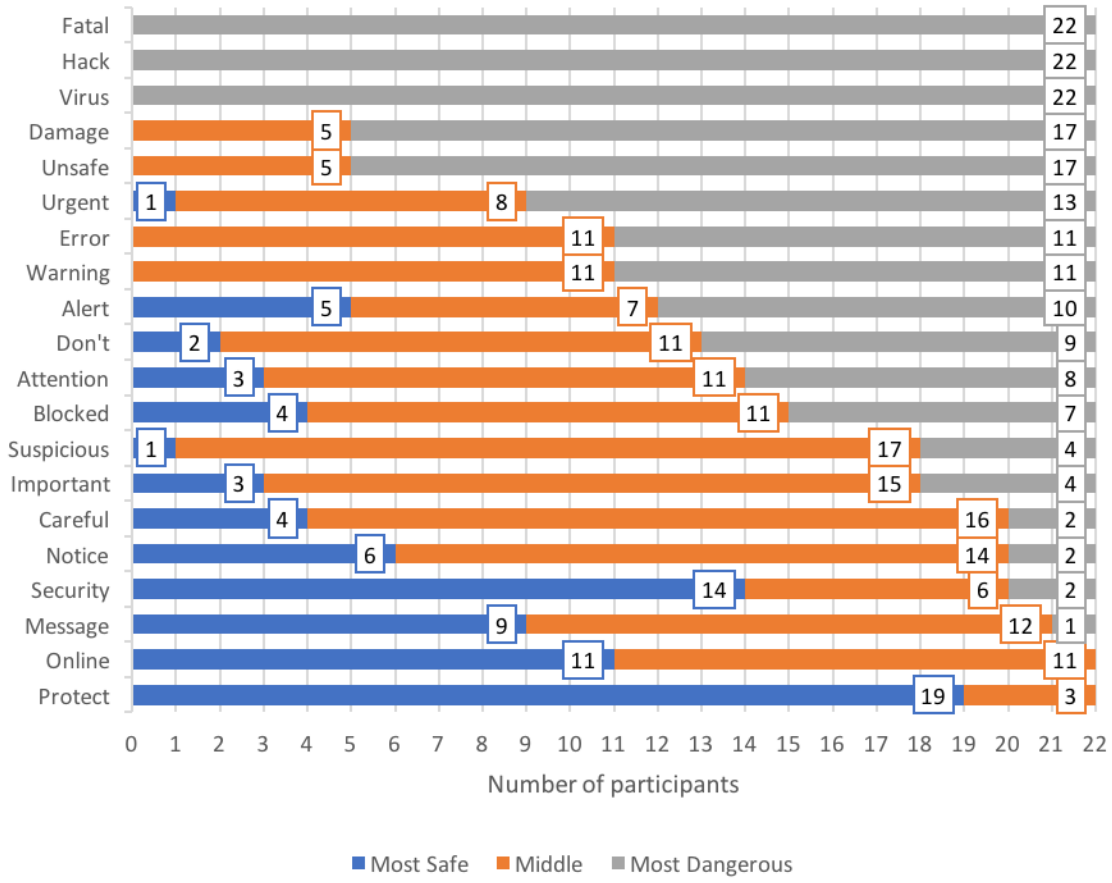


Figure 4.4: Number of children placing words in each severity category.

more than half of the children believed that it was nevertheless difficult to classify symbols (n=13, 59%) due to reasons such as: difficulty understanding the symbols, uncommon symbols for warning messages, lack of experience seeing some of the symbols online, different implications of a symbol and multiple symbols that are similar to one another.

Categorization of Signal Words

Figure 4.4 illustrates the categorization of words.The word *protect* was considered most safe (n=19, 86%) while the words *fatal*, *hack* and *virus* were unanimously considered most dangerous (n=22, 100%).

According to the participants, words were less difficult to categorize than colours

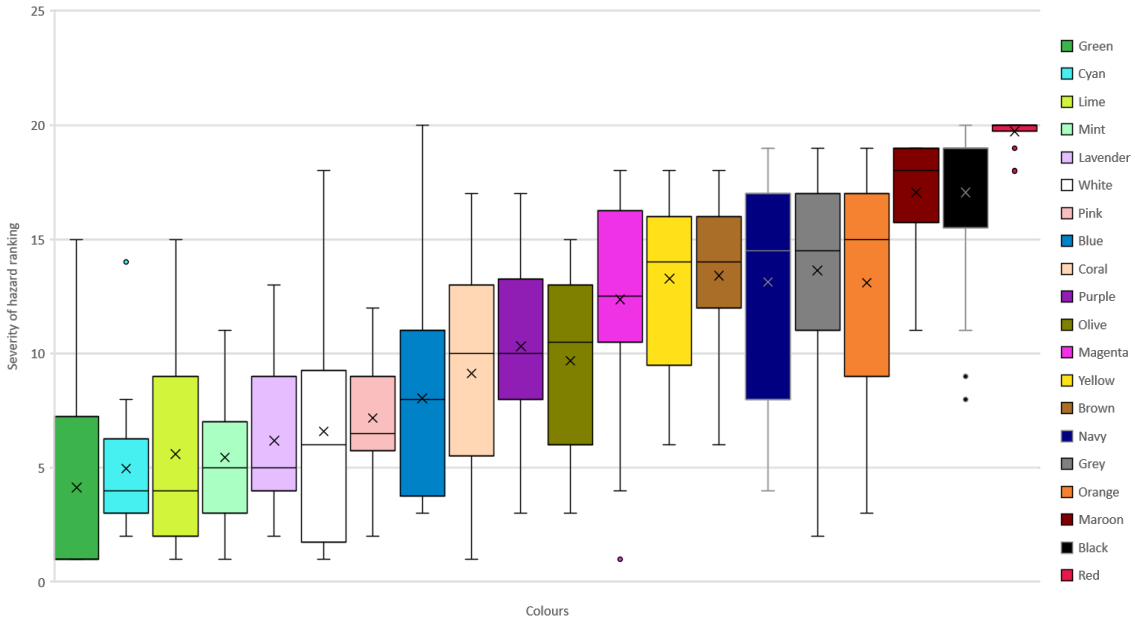


Figure 4.5: Children's ranking of colours sorted by median rank, where rank 1=most safe and 20=most dangerous.

but more than symbols (n=14, 64%). Many children felt that there was more ambiguity in classifying the words because of the lack of context or explanation when using only words, multiple meanings that a word may carry, uncommon words for warning messages, lack of experience seeing some of the words online and multiple words that are similar to one another.

4.2.2 Card Ranking

Following the categorization, participants were asked to rank the cards placed in each category to give participants a smaller set to work with at a time, starting from the most safe item to the most dangerous item. We numbered the overall ranks from 1 to 20, by ordering the items from each category (most safe, middle, most dangerous) sequentially for each participant. All responses are summarized using box and whisker plots, which illustrates the distribution of data and its variability based on the five-number summary: minimum, first quartile, median, third quartile, and maximum. The individual plotted points represent outliers. We first present the results of colour hazard ranking.

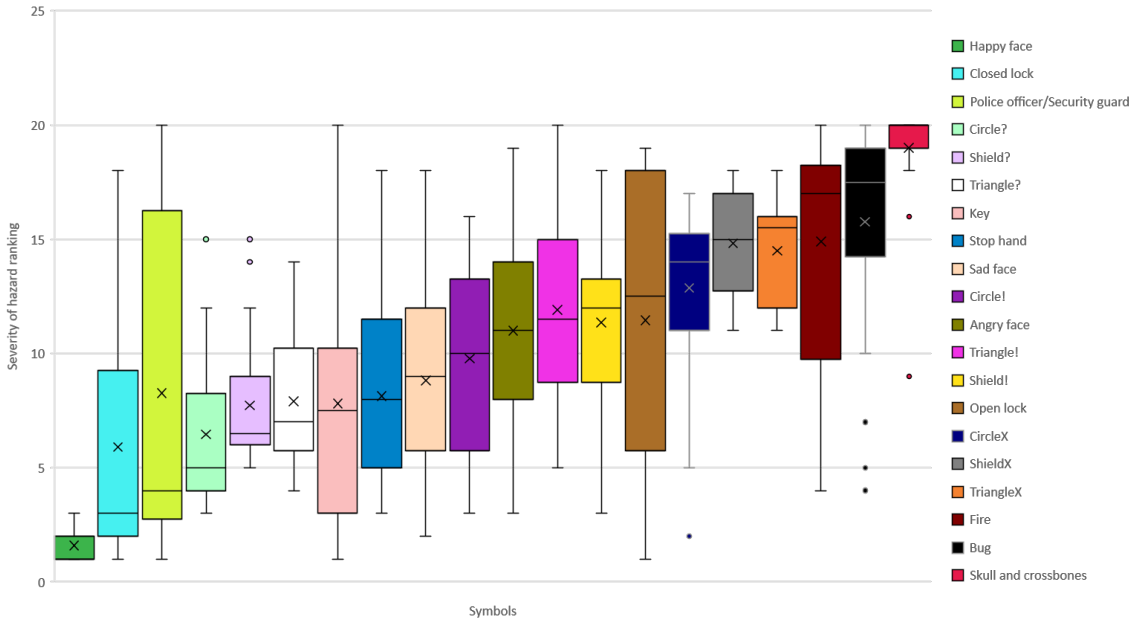


Figure 4.6: Children's ranking of symbols sorted by median rank, where rank 1=most safe and 20=most dangerous.

Hazard Ranking of Signal Colours

Figure 4.5 represents the colour hazard ranking. Similar to the colour categorization (Figure 4.2), we see that *green* was considered the most safe colour while *red* was considered the most dangerous. Children had a really high level of agreement on the hazard ranking of the colour *red*: many considered it the most dangerous colour (rk=ranking=20, m=median=20). Some colours (e.g., *cyan*, *mint*, *pink*, *brown*, *maroon* and *black*) had moderate amount of variability, while others (e.g., *green*, *lime*, *white*, *blue*, *coral*, *olive*, *yellow*, *navy* and *orange*) had a higher variability in their hazard ranking.

Hazard Ranking of Signal Symbols

Figure 4.6 illustrates the symbol hazard ranking. More than half of children agreed on the hazard ranking of the extremes such as the *happy face* (rk=1, m=1) and *skull and crossbones* (rk=20, m=20). Symbols such as the *police officer/security guard* and *open lock* had the most variability.

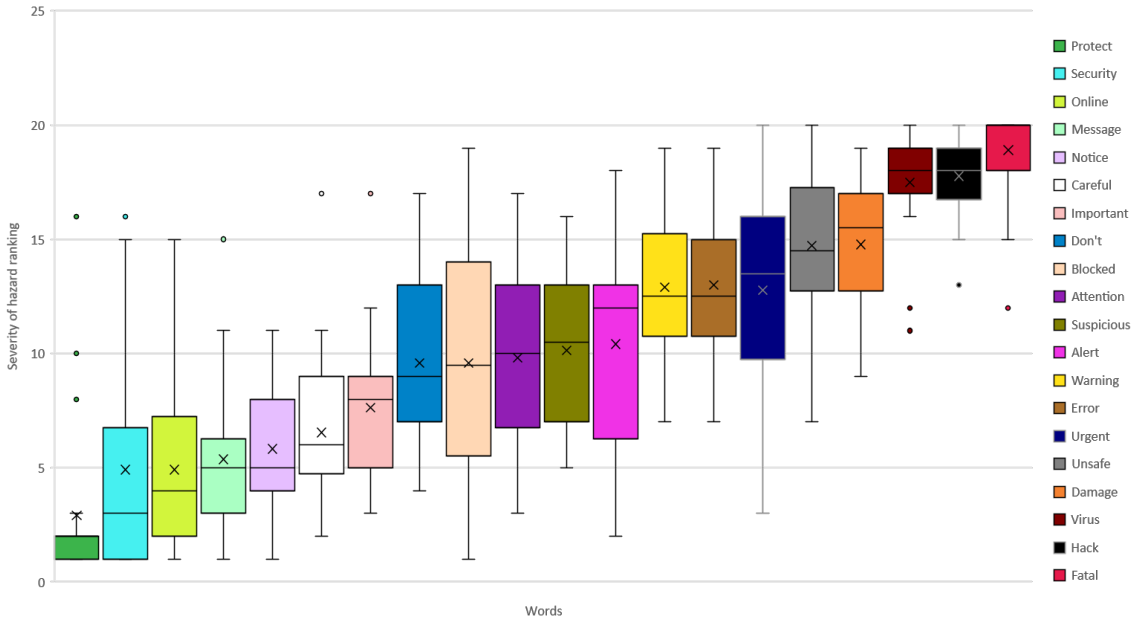


Figure 4.7: Children's ranking of words sorted by median rank, where rank 1=most safe and 20=most dangerous.

Hazard Ranking of Signal Words

Figure 4.7 summarizes the word hazard ranking. Generally, some participants agreed that the word *protect* was the safest (rk=1, m=2) and the words *virus* (rk=18, m=18), *hack* (rk=19, m=18) and *fatal* (rk=20, m=20) were dangerous. Words such as *blocked* and *alert* had the most variability.

4.2.3 Qualitative Themes from Card Categorization and Ranking

The participants used the think-aloud protocol as they sorted and ranked the cards. Participants' comments were recorded and transcribed. Figure 4.8 represents children's most frequently used terms when describing colours, symbols and words. The participants most often used terms such as "dangerous", "safe", and "warnings".

We extracted 572 excerpts for colours, 458 for symbols and 454 for words. These excerpts were coded under 7 major themes that we identified during the content analysis (Section 3.7.2) 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.

Figure 4.8: Word cloud to visualize children's most frequently used terms when describing colours, symbols and words.

Themes are not mutually exclusive and therefore, one excerpt may be coded under multiple themes.

Signal Colour Themes

We summarize the top 3 most discussed colours and the top theme with most excerpts. Figure 4.9 summarizes the distribution of the excerpts for colours. The most discussed by participants were *black*, *red*, and *green* and *white*.

Black was associated with the *level of danger* (*ne*=n excerpts=9). It was mostly seen as a dangerous colour (*ne*=7) and sometimes as a safe colour (*ne*=2). Participants' *previous experience* (*ne*=3) with *black* was a factor in determining its associated severity of hazard. *Black* was significantly coded under *subjective perception*

Colour themes	Ambiguous	Association with colours/hues	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Black	1	8	2	3	9	7	12	42
Blue		9	2	3	7	5	4	30
Brown	1	8		1	6	3	3	22
Coral	4	13			3	3	3	26
Cyan		9		1	4	5	7	26
Green		7	1	2	7	16	5	38
Grey		11	1	2	5	5	5	29
Lavender	1	10	1	1	4	4	4	25
Lime		9		1	6	5	4	25
Magenta	1	13			1	2	3	20
Maroon		13			3	2	3	21
Mint		14			3	3	7	27
Navy	1	11	2	3	6	2	4	29
Olive	1	13		1	4	5	3	27
Orange	2	7	1		5	4	2	21
Pink		9	1	2	5	6	6	29
Purple	3	9		1	5	3	7	28
Red		6	6	3	6	12	7	40
White	5	8	1	2	6	8	8	38
Yellow	2	2	1	2	8	10	4	29
Total	22	189	19	28	103	110	101	572

Figure 4.9: Number of excerpts distributed across themes for colours. Orange = Most frequent theme per colour, ▫ = Most frequent colour per theme.

(*ne*=12). For example, children considered *black* to be negative (*ne*=5) because it reminded them of "black holes [that] are scary and not safe" (**C17**), and because "[the] darker the colour, the worse it is" (**C22**). Children also believed that *black* was common (*ne*=4), as participant (**C04**) pointed out, "black would be dangerous but I see it so many times, it's not very effective." They also perceived it to be attention grabbing (*ne*=2) because *black* is a "darker colour and it stands out" (**C18**).

Participants regarded *red* to be most closely *associated with other parameters* (*ne*=6), such as symbols like "fire" (*ne*=2). Children discussed *red* through *contextual associations* (*ne*=12) such as road signs and lights (*ne*=7) and technology (*ne*=3).

The following quotes are some examples of contextual associations that were made by the participants:

> "It's on a stop sign, it's red, something bad is going to happen." **C20**

> "Most websites trying to scam people have red backgrounds. Every time I go to a website that has a warning, it has [a] red background. Those are the scamming ones." **C11**

Children discussed *green* using various *contextual associations* (*ne*=16) related to road signs and lights (*ne*=6), technology (*ne*=5), nature (*ne*=2) and social conventions (*ne*=2):

> "I thought of mainly street lights, green is go so it's safe to go, kind of what I did with all green's, like lime, olive, mint." **C07**

> "Because [green] is just like [saying] everything is okay, check your computer, and if it's all upgraded, and it says all good, it will be green. Something [that is] minor wrong, it will be yellow, and if it's bad, then red." **C12**

Interestingly, children generally believed that *white* was *ambiguous* (*ne*=5) due to the colour being "neutral", "empty" and "blank":

> "[White is an] empty colour, nothing dangerous. It's not really a colour, it's not dangerous." **C10**

> "[White is] not really a colour, it's just blank, people might think there's something wrong. It's not as safe as vivid colours." **C12**

The majority of colours were coded under the theme, *association with colours and hues* (*ne*=189), because children most soften described colours in relation to other colours. They believed that many of the colours showed similarities with other colours (*ne*=117). For instance, the colour *mint* (*ne*=9) reminded participants of "green", "cyan", "blue", "lavender", "lime" and "coral". They were associated with dark colours (*ne*=44), such as navy (*ne*=7). They had differences with other colours (*ne*=22), such as *white*, which was described as apart from all other colours (*ne*=4).

Symbol themes	Ambiguous	Association with symbols	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Angry face	1	2			3	9	12	27
Bug	2		4		4	11	6	27
Circle!	1	3	2	1	1	4	4	16
Circle?	7	2	2	1	2	2	3	19
CircleX		6		1	5	5	4	21
Closed lock		2	2		6	11	3	24
Fire	2	1			6	11	5	25
Happy face		4		1	5	5	10	25
Key	1	4	1	1	1	13	4	25
Open lock			1		2	14	3	20
Police officer or Security guard			2	1	7	14	7	31
Sad face		3			5	4	8	20
Shield!		6	2	1	6	6	2	23
Shield?	4	2	1	1	5	9	2	24
ShieldX		5	1		3	4	4	17
Skull and crossbones		1	1		6	19	8	35
Stop hand	1	1			2	10	4	18
Triangle!		3	2	1		6	3	15
Triangle?	4	1	1	1	5	8	4	24
TriangleX	1	5	3	1	3	4	5	22
Total	24	51	25	11	77	169	101	458

Figure 4.10: Number of excerpts per theme for symbols. Orange = Most frequent theme per symbol, □ = Most frequent symbol per theme.

Signal Symbol Themes

The distribution of the excerpts for symbols is summarized in Figure 4.10. The most discussed symbols were *skull and crossbones*, *police officer or security guard*, and *angry face* and *bug*.

Children believed that *skull and crossbones* (*ne*=19) was dangerous and most associated with warning labels (*ne*=11) and technology (*ne*=7):

> "I see [skull and crossbones] on bottles, it's something toxic, I would ask my parents to use it for me, to help me with it." **C10**

> "[Skull and crossbones] looks like poison, if you go on, poison will dissolve on your computer, it won't work anymore." **C16**

The symbol *police officer or security guard* was discussed using *contextual associations* (*ne*=14) related to technology (*ne*=10). It was also commonly seen as conveying the *level of danger* (*ne*=7). Some thought it was both safe and dangerous (*ne*=4), while others saw it as simply dangerous (*ne*=3):

> "[Police officer or security guard] can be safe and dangerous. It protects that website from hackers but if you say rude or inappropriate comments [about the] website, the security guard or police officer can find you with your email." **C12**

> "I'd feel unsafe like my data might have leaked or something, something dangerous is happening." **C14**

Angry face was notably associated with *subjective perception* (*ne*=12), where the participants considered it to be predominantly negative (*ne*=11):

> "If you see someone yelling, in general, you don't feel safe. When people are upset, they can do bad things, it's warning you that there might be some bad things." **C12**

Children described *bug* in terms of *contextual associations* (*ne*=11) such as technology (*ne*=10). Interestingly, *bug* was *associated with other parameters* like the word "virus" (*ne*=4).

> "[Bug] is like a virus, or [it is saying] something's wrong. Difference between virus and a bug [is that] virus is [when] something or someone else do something to your computer, and bug is something not working like it should." **C06**

All symbols were described using *contextual associations* (*ne*=166) related to technology (*ne*=133), warning labels (*ne*=16), media (*ne*=8), social conventions (*ne*=8) and road signs and lights (*ne*=4).

Word Themes	Ambiguous	Association with words	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Alert		8	2		3	6	3	22
Attention		6			6	5	3	20
Blocked					8	16	5	29
Careful	1	2	1		8	5	2	19
Damage					1	13	7	21
Don't				1	3	7	4	15
Error		1		1	2	10	6	20
Fatal		4			6	10	8	28
Hack		2			2	16	6	26
Important		3		1	4	8	1	17
Message		4			7	12	4	27
Notice		3			5	11	4	23
Online	2			2	8	14	4	30
Protect	1	4	1		2	10	6	24
Security		5			5	8	5	23
Suspicious	1	2			3	11	7	24
Unsafe		1			11	9	2	23
Urgent		3			5	7	3	18
Virus	1		1	2	4	12	4	24
Warning		3		1	5	9	3	21
Total	6	51	5	8	98	199	87	454

Figure 4.11: Number of excerpts per theme for words. Orange = Most frequent theme per word, □ = Most frequent word per theme.

Signal Word Themes

Figure 4.11 summarizes the distribution of the excerpts for words. The most discussed words were *online*, *blocked* and *fatal*.

Online was seen as *ambiguous* and "unclear" (*ne*=2), mostly influenced by participants' *previous experience* (*ne*=2) compared to other words. Children discussed *online* using *contextual associations* related to technology (*ne*=14):

> "If I am not with my friends and family, I can contact them online, sometimes it's a private chat so that you can talk to just them." **C09**

> "[Being online] could be safe, but it's where a lot of cyberbullying happen." **C13**

In particular, participants believed that the word *blocked* (ne=16) was closely related to *contextual associations* such as technology (ne=14) and media (ne=2):

> "[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**

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

> "[It's like] blocking people on social media." **C05**

Fatal was associated with *subjective perception* (ne=8), in which the participants considered the word to be very negative (ne=8):

> "[Fatal means] something really bad will happen. [something] very dangerous [is] on your device, it can completely crash your entire computer." **C15**

Like colours and symbols, all the signal words had excerpts describing *contextual associations* (ne=199) such as technology (ne=182), media (ne=10) and social conventions (ne=7).

4.3 Post-test Semi-structured Interview

During the post-test semi-structured interview, we asked participants open-ended questions regarding their online activities, attitude towards, and previous experience with, cybersecurity warning messages, and what they would expect to see on such warnings.

We coded the post-test excerpts by themes for each interview question. There may be multiple excerpts per participant and these may be allocated to multiple themes if applicable.

4.3.1 Definition of "Cybersecurity Warning Message"

For the purposes of this research, we use the definition of warnings outlined in Section 2.2, which are based on different types of communications relevant to security tasks from Cranor's HITL framework [13]. Our research focuses specifically on security *warning dialogs* and *notices*.

When the participants were asked to define warning messages, almost all children were able to give reasonable definitions. Nineteen participants defined cybersecurity warning messages as *warning dialogs* actively suggesting ways to help users avoid or mitigate a hazard:

> "When you are on a website and playing online game that someone created, a little thing in the middle pops up with symbols, it could say, 'Hey watch out, this website has something dangerous on it or a bug, if you don't want it or not want anything to happen, you should get out'." **C17**

> "Sort of [messages] that come up to warn you to don't give out your information, or download this to protect your computer." **C22**

One participant saw warnings as *status indicators*, passive messages that inform users about a system status without necessarily asking users to take action:

> "Warning that will show up on your screen on any device that you are on, says that something is wrong, or if you updated or uploaded something, it will say everything is okay. Sometimes, it will be in different colours for different messages." **C09**

One participant noted that warning messages could be *phishing scams*, which trick users in providing sensitive information:

> "If you see these messages, don't click them, just close all the tabs or whatever you are on and try going on Internet again or just do not do what it says. They mostly try to put virus in your computers, some of them try to hack your accounts or hack your Google account, or trying to scam people or get their information." **C11**

4.3.2 Attitude Towards Cybersecurity Warning Messages

Children had various opinions on the positivity or negativity of warning messages. Twelve participants interpreted warnings as something *both* positive and negative. Generally, the warnings were perceived *positive* when they alert users of a threat, explain the risks and consequences, or confirm the safety of the activity. On the other hand, warnings were considered *negative* when they are fake, phishing messages, give viruses or interrupt users' activity. The following are some of the participants' comments:

> "Positive - you are not allowed to watch, [it's] letting you know that it's being hacked [or is a] virus protection. Negative - [it's] warning you [of] something not true, you should get virus protection." **C04**

> "Both, it depends. You can get mad and you can get relieved and be happy that you know. I prefer having a warning message show up, but depends if I have one in the middle of the game for example, but I would prefer one." **C08**

> "Both. It can tell you things are safe, and everything is okay. It can also tell you if you are not doing the right thing, or if you are doing bad stuff on purpose, there might be those cyber messages that come up and say you are doing inappropriate stuff, or there might be a police officer photo thing and they are saying if you keep doing it, the police might have to get involved." **C12**

Five participants found warning messages to be only *positive*:

> "Positive - so that kids will know that it's bad to do this or good to this, [it] is never a negative thing." **C10**

> "It's a good thing because it's a warning, it helps you more than when computer don't tell you when someone hacks you." **C21**

Contrarily, four participants believed warnings to be only *negative*:

> "Negative. [They] get people to confirm email or take money PayPal, virus or a way of someone to hack, getting little kids to give information to the people." **C01**

> "Negative - I don't like seeing them because they are trying to get my attention to go to their website or download things that will make [a] virus. It doesn't make me feel good." **C11**

Those viewing warnings as negative misunderstood the term and instead associated warnings with malicious intentions.

4.3.3 Type of Cybersecurity Warning Messages

During the interview, participants were asked to share a story about their previous experiences with cybersecurity warning messages. Through their storytelling, we were able to gather information on what they were doing prior to receiving warning messages, what type of warnings they encountered, their reactions to the messages and if they told anyone about them.

Prior to receiving warnings, children were generally watching YouTube videos, playing games, browsing the web, downloading files or using social media. Nine participants encountered *pop-ups* during an activity:

> "I was on my mom's iPad, looking online, a message popped up and it only had a 'Yes' and no 'No' option." **C13**

Five participants encountered *system status* indicators that they interpreted as a security warning, five encountered *virus* warning messages and five came across *censored* content messages:

> " The [warning message said,] iPad needs to be backed up." **C04**

> "At school on my PC, I was doing classwork on Google docs, all of a sudden something pops up [like a] firewall but bigger, saying there was a virus." **C08**

> "[On] Instagram, my friend wanted to show me something, a weird cool video thing and it seemed really interesting, and there were a lot of pictures that were blurred out, and a message that said, 'This picture or video has some disturbing content, double tap to see photo'." **C12**

Four participants experienced *phishing* messages:

> "I used Firefox, and it gave me alert message, turns out it was a scam. [It said,] 'Warning, you are in danger, you must pay this much'. I just asked my dad and he said it was a scam, we just closed the browser." **C19**

Three children found the messages to be *educational*:

> "When I was younger, I played a game called MovieStarPlanet. In the beginning when making [an] account, you have characters and [you] make a video - [there was a] warning message in a video [where] the guy asked him what his password was and he hacked him. [It said] don't give people your password, be safe online." **C02**

Two participants believed that the warnings provided *actionable advice* such as providing instructions or a number to call:

> "[My] first time with a warning message [was when the] computer [was] heating up. [I saw] ! With yellow [symbol], a week after getting [the] computer...It was telling me to shut off [the] computer. It's good that it told me but it wasn't a good thing that my computer was heating up." **C06**

Two children came across *ads*:

> "I was browsing the Web and then I found a thing I wanted to download, it brought me to a website, AdFly, and under it, it showed an ad which was a warning message (it was counting down at the top and when it reached zero it said to skip ad) so I thought it was fake." **C14**

4.3.4 Reactions to Cybersecurity Warning Messages

Children were also asked about what they did after encountering warning messages. Three quarters of children (n=16) reported that they *received help* from others and another three quarters (n=16) reported that they *actually read* the messages:

> "Read it, and if it is a virus, I would call my uncle, he would just walk over to check it out." **C08**

> "I would read it, think of what I should do, if it's something that is hard I would ask [if] anyone could help me." **C09**

Approximately half of the participants (n=12) mentioned that they *continued with the activity by going around* the warning message. They did so by ignoring the message, dismissing, closing or exiting the pop-up window, tab or the website:

> "I just close out all the tabs. I ignore the warning and just close it sometimes when it doesn't seem too dangerous." **C11**

Three participants *stopped the activity*, three *turned off and restarted the device* and three *continued with the activity after clicking* on the warning message:

> "If it's really bad then I go tell someone. If it is a mild one and says you can see the picture, I don't look at the disturbing picture or go to the website." **C04**

> "If there is an X, I would just remove it, and if it doesn't close, I would close the tab or restart the computer." **C22**

> "If it has a 'yes' or 'no' option, I usually press 'no'. If it asks, 'Would you like to update?' I say 'no'. I click whichever option is not 'yes', so 'no', 'ignore', 'dismiss' or the 'X' on the window." **C13**

Two participants *deleted browsing history* and one participant *ran a malware scanner*:

"They said to delete the search history to delete [virus] and I'm not sure if it's been deleted, but it seems like it has been." **C13**

"If it looks real, I read it some more, and if it looks really dangerous, I use malware bites and scan the computer." **C14**

4.3.5 Reporting Habits for Cybersecurity Warning Messages

Almost all participants talked to someone when they encountered cybersecurity warning messages. Most children (n=19) reported to an *adult*, primarily a parent. Other adults included older siblings and teachers. Three children told their *friends* and two received *professional help* from the Apple store. Only two children said they *did not report to anyone* because they already knew what the messages meant and how to deal with them.

Some children clarified that they perform preliminary triaging and that they would show the warning messages to adults when they are dangerous, difficult to understand or out of their control. An adult was viewed as someone capable of handling these types of suspicious situations that are beyond the children's comfort level:

"Yes, if it is too dangerous, I will tell my friends or my mom and dad." **C11**

"If a message is really bad, I'd show an adult. I wouldn't show my friends because they're my age; they might react differently than an adult, and an adult might actually know what to do." **C12**

"I would show it to my dad if I thought it was dangerous." **C14**

"Yes if I didn't understand it, I would definitely call an adult to help me." **C21**

"I would show it to adults if it is dangerous." **C22**

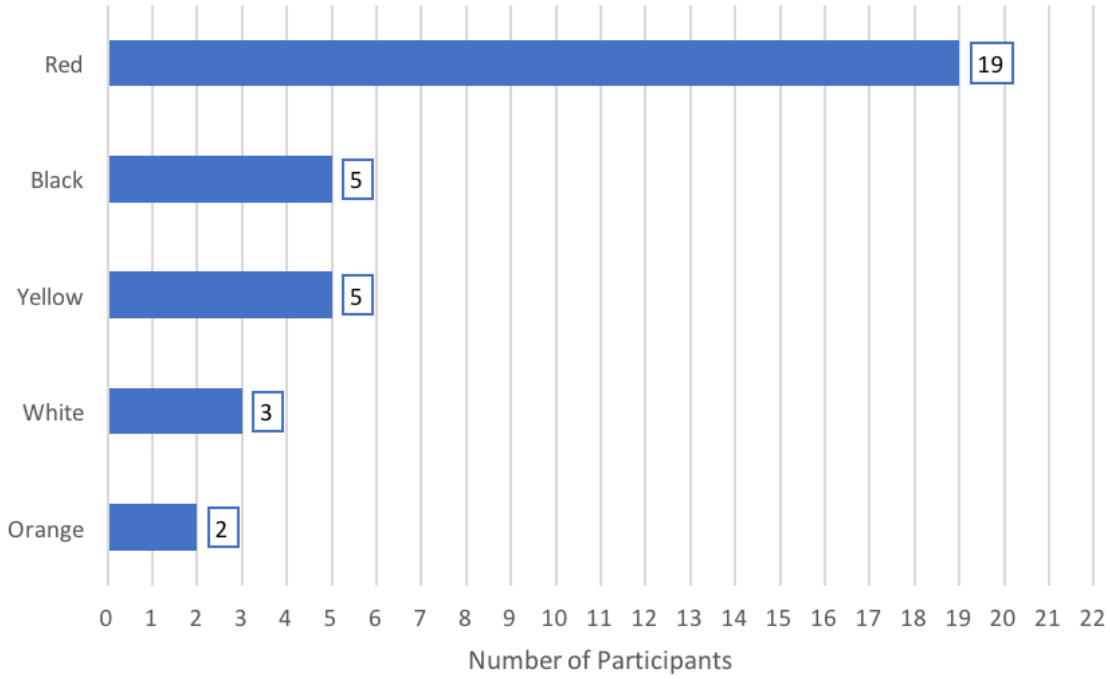


Figure 4.12: Children's expectations for cybersecurity warning messages for colours.

4.3.6 Children's Expectations for Cybersecurity Warning Messages

At the end of the interview, we asked the participants what they expected to see on cybersecurity warning messages to indicate something dangerous. All participants gave comments on the type of warning design parameters they would expect. This was unsurprising given that they had been primed by the categorization and ranking activities, but it nonetheless provides insight into these particular parameters.

Colours

Figure 4.12 summarizes children's expectations for colours. Most participants (n=19) expected to see the colour *red*, highly surpassing the other colours.

Some interesting suggestions included less frequently mentioned colours such as *grey* and *blue*. Participant **C22** mentioned "spots of grey and background is black", referring to the black-and-white static that you may see on TV. Participant **C12** wanted blue, "like a blue screen of death". Other noteworthy comments pertaining

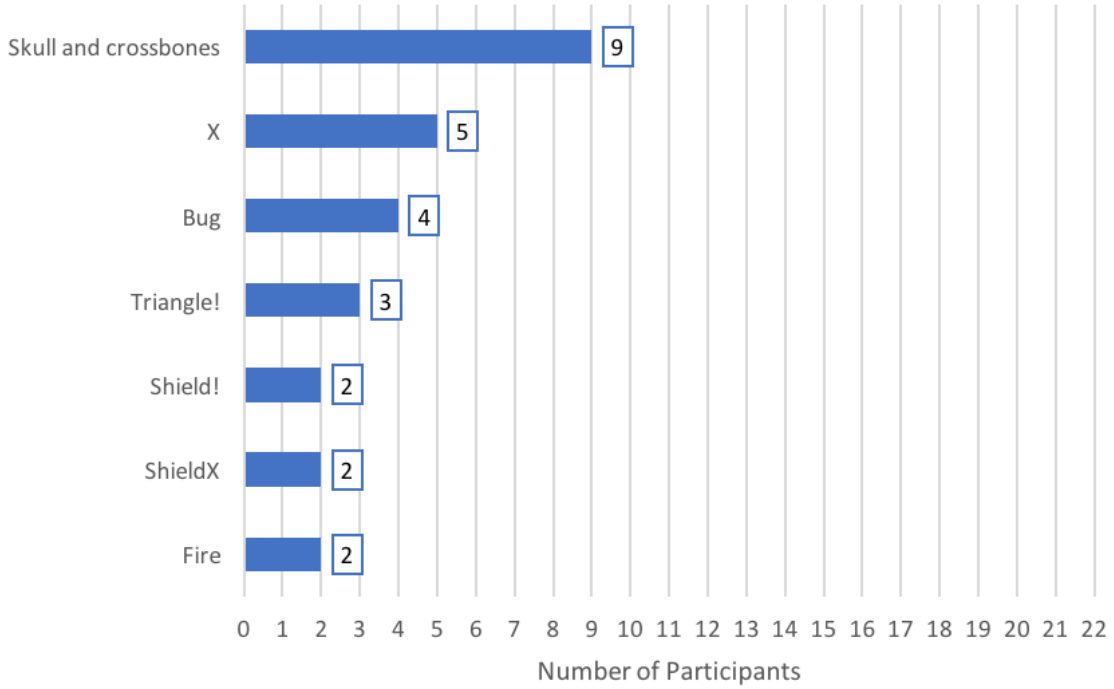


Figure 4.13: Children's expectations for cybersecurity warning messages for symbols.

to colours included different, flashing and random colours:

> "It will be cool to have these different colours on warning messages." **C02**
>
> "I would put flashing colour like TV you know how when old TVs don't work, random colours pop up." **C13**

Symbols

There was less agreement for symbols, as shown in Figure 4.13. Nine participants expected to see *skull and crossbones* on dangerous warning messages, followed by the symbol *X* (n=5) or a *bug* (n=4).

Some participants mentioned symbols outside of the 20 signal symbols used for categorization and ranking, such as a "caution tape" (**C04**), a "guy wearing hood in front of the computer" (**C17**), a "computer symbol with X" (**C22**) and an "evil maniac" (**C20**). Each of these are recognizable as representing "danger" in other circumstances.

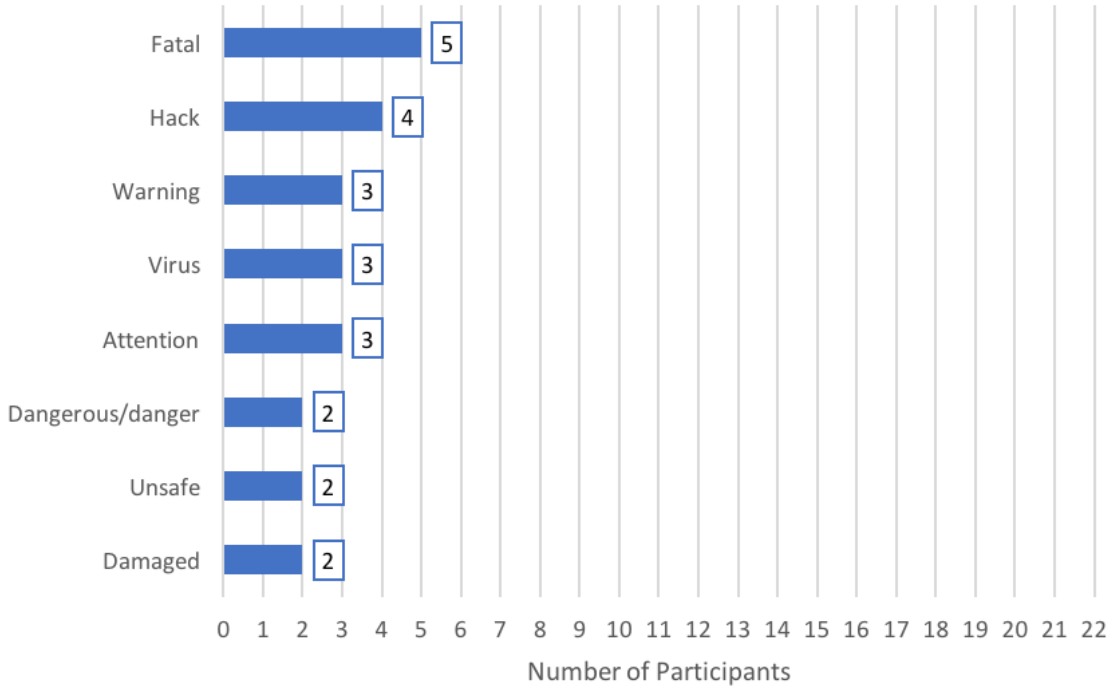


Figure 4.14: Children's expectations for cybersecurity warning messages for words.

Words

Figure 4.14 illustrates children's expectations for words. There were fewer suggestions relating to expected words. Five participants expected to see *fatal* on warning messages.

Most children expected to see several signal words per warning message. Participant (**C17**) offers this example using the words *hack* and *bug*: "You are getting hacked at the moment, there is a bug in the process of downloading."

Other Characteristics

Most children enthusiastically provided additional suggestions for effective warning messages. From their explanations, we identified seven trends summarized in Figure 4.15.

Children mostly emphasized the importance of visual cues to signify that the warning is important and worthy of attention. They suggest *bright and flashing*

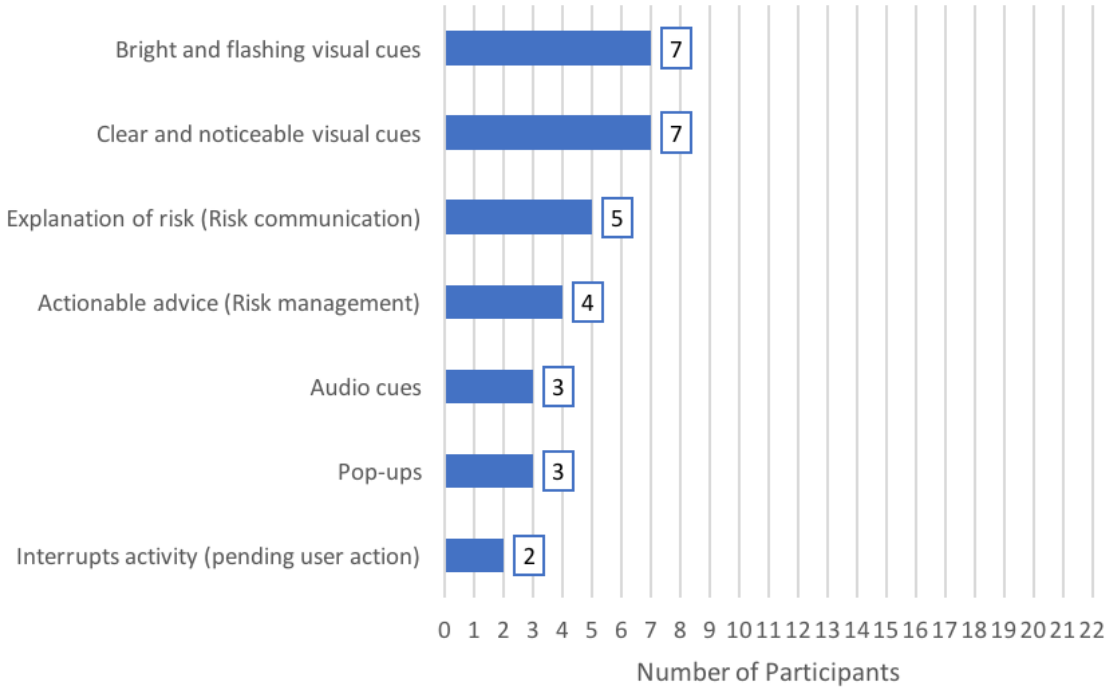


Figure 4.15: Children's expectations for cybersecurity warning messages for other characteristics.

(n=7) and *clear and noticeable* (n=7) messages:

> "For a kid, big with big image (sad face or X mark), say tell your parents, white and red, also bright colours because your eyes look at those first." **C08**

> "I would put flashing colour like TV." **C13**

> "[A] big warning message is more important, [a] tiny icon doesn't seem important." **C04**

> "Font really readable, big and bold." **C18**

Some participants suggested including more information concerning risk communication and management at a child-appropriate level. For example, they wanted messages that provide an *explanation of the risk* (n=5) and *actionable advice* (n=4) 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**

> "Put you in the new tab and say what was happening. [Have a] pop-up that explains what happened." **C17**

> "...a little message on what you should do." **C20**

The remaining suggestions pertained to interrupting the user to ensure that the warnings receive the user's attention. They proposed *audio cues* (n=3), *pop-ups* (n=2) and *activity interruptions pending user action* (n=2):

> "Make the alarm go off, not too loud, making some kind of noise to tell you to get off the website." **C16**

> "It would pop up big on my screen, open up a new window. I would notice it this way." **C14**

> "...make sure you can't exit off the tab until it is solved." **C08**

4.4 Summary

Consistent with literature on warnings with adults [3, 16, 25–28, 36, 39, 64], we found that children had similar notions about what design parameters would constitute dangerous or safe warning messages. Children believed that *red*, *skull and crossbones* and *fatal* were considered most dangerous, while *green*, *happy face* and *protect* were the most safe. Our findings suggest that children determined the severity of hazards for colours, symbols and words based on *contextual associations*, perceived *level of danger* and *subjective perception*. Children's expectations for warnings that communicate danger were consistent with the items they ranked most dangerous. They also suggested other design characteristics like *visual cues that are bright, flashing, clear and noticeable*.

Chapter 5

User Study with Adults

We repeated the study with adult participants, testing the same signal colours, symbols and words as in the children's study. The findings will help us understand children's responses in comparison to the current baseline and will help us determine design guidelines for effective warning messages for children.

5.1 Participants

We recruited 22 adult participants for the second study. This number is consistent with our children's study and Fugard and Potts' [23] suggested sample size for thematic and content analysis.

Table 5.1 summarizes the participants' demographics. The 22 adult participants were between the ages of 18 to 51, with an average of 27 years (SD=8.06). There were 10 males and 12 females. Nine participants were currently enrolled in or had a Bachelor's degree, eight had a Master's degree, four had a Doctorate degree, and one had some college credit with no diploma. All participants were online daily for an average of 8 hours and 15 minutes (SD=5.15). Adults used various devices to go online and the most popular devices used were desktop (n=22) and laptop computer (n=22), followed by iPhone (n=17), Android phone (n=17) and iPad (n=17), gaming consoles (n=15), other tablets (n=12), Blackberry (n=9) and Windows phone (n=4). All adults (n=22) had experience in using more than one device to go online.

The adults engaged in various online activities summarized in Figure 5.1. Adults regularly used *SNS* such as Facebook, Instagram, Twitter, Snapchat, WhatsApp, Telegram and Tinder. The majority of participants regularly went online to access

ID	Sex	Age	Education	Days/week	Hours/day
A01	Female	24	Bachelor's	7	5
A02	Male	26	Some college, no diploma	7	17
A03	Male	31	Doctorate	7	4
A04	Female	29	Bachelor's	7	15
A05	Female	51	Bachelor's	7	3
A06	Male	28	Doctorate	7	10
A07	Male	28	Doctorate	7	5
A08	Male	28	Master's	7	2
A09	Female	23	Master's	7	11
A10	Female	26	Master's	7	6
A11	Female	26	Master's	7	10
A12	Male	19	Bachelor's	7	8
A13	Male	31	Bachelor's	7	5
A14	Male	48	Master's	7	4
A15	Female	28	Doctorate	7	10
A16	Female	22	Bachelor's	7	14
A17	Female	25	Master's	7	8
A18	Female	22	Master's	7	3
A19	Female	19	Bachelor's	7	14
A20	Male	26	Bachelor's	7	2
A21	Female	23	Master's	7	20
A22	Male	18	Bachelor's	7	5

Table 5.1: Adult participant demographics.

email and *media* (e.g., YouTube, Netflix, Reddit, Buzzfeed, daily news, sports). Some participants also used a *search engine* such as Google for web-browsing.

We observed two activities for adults that were not observed in children. Half of participants mentioned that they went online for *professional and educational* purposes (e.g., LinkedIn, Indeed, library databases, cuLearn (Carleton's Learning Management System)), and a few went online for *personal* activities (e.g., online banking, travel, shopping).

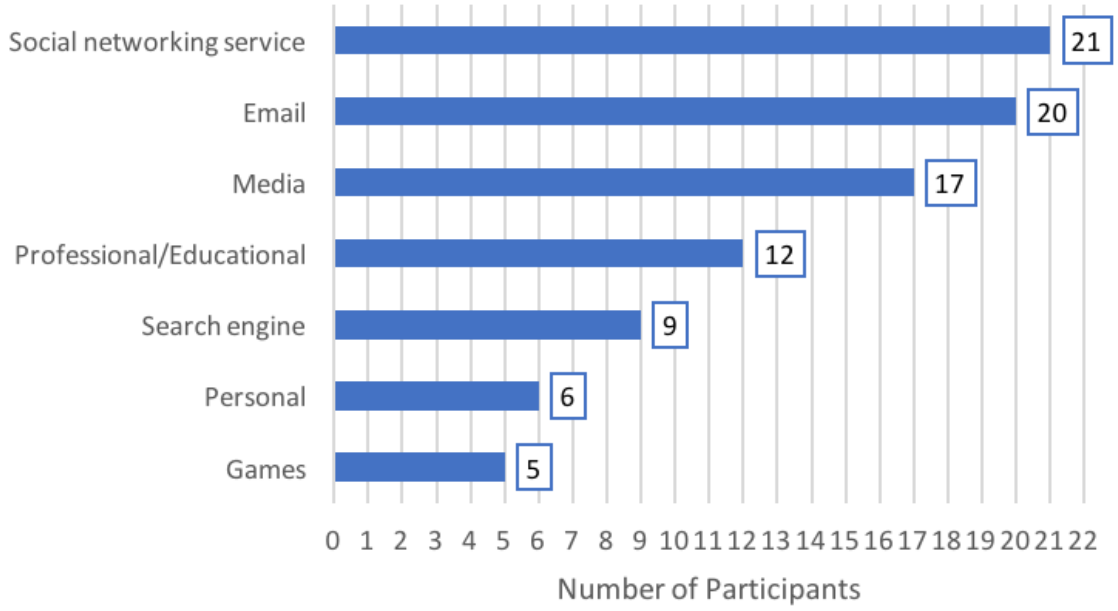


Figure 5.1: Adults' online activities.

5.2 Results

We discuss results from adults' card categorization and ranking, qualitative findings, and post-test semi-structured interviews.

5.2.1 Card Categorization

Participants categorized cards for colours, symbols and words into the most safe, middle, and most dangerous categories.

Categorization of Signal Colours

Figure 5.2 illustrates the categorization of colours into three severity categories. Similar to the results for children (Section 4.2.1), *green* was considered the safest (n=18, 82%) while *red* was most dangerous (n=21, 95%). Most lighter and cooler shades were considered safer while darker shades and the colours indicating "stop" on traffic lights and signs (e.g., red, yellow) were seen as more dangerous.

During the interviews, adults mentioned difficulty categorizing the colours (n=17,

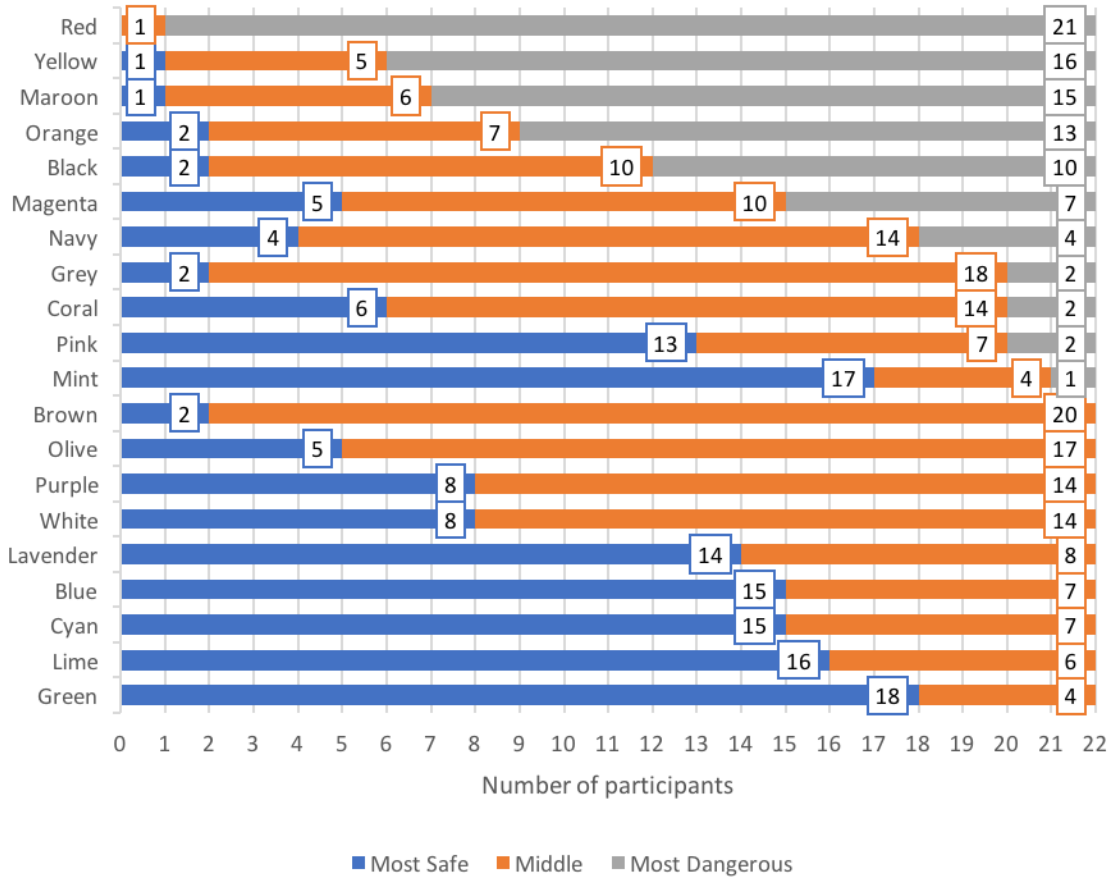


Figure 5.2: Number of adults placing colours in each severity category.

77%) due to a lack of context or explanation when using only colours, seeing uncommon colours for warning messages and how subjectivity affects the perceived hazard.

Categorization of Signal Symbols

Figure 5.3 depicts the categorization for symbols. The majority of participants believed that *happy face* was considered most safe (n=21, 95%) and *skull and crossbones* was most dangerous (n=20, 91%). Similar to children, we observed that adults were less likely to categorize symbols as safe. Some symbols had high categorization variability, specifically those that were common in security warning messages (i.e., *open lock*, *police officer/security guard* and *stop hand*). Contrarily, we observed that symbols relating to hazardous materials (i.e., *skull and crossbones* and *fire*) were

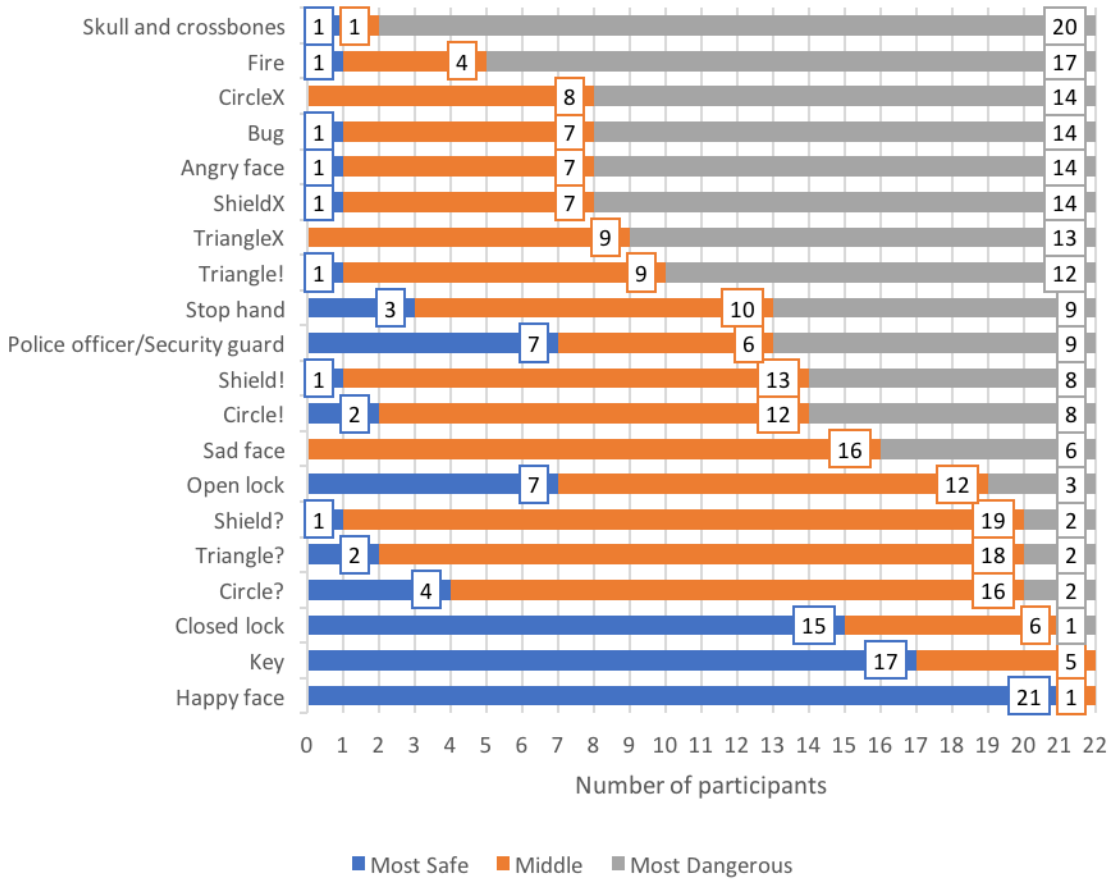


Figure 5.3: Number of adults placing symbols in each severity category.

considered dangerous.

Adults believed that symbols were second most difficult to categorize (n=15, 68%), due to: finding them to be uncommon symbols for warning messages, difficulty understanding the symbols, seeing multiple symbols that are similar to one another, having different implications of a symbol, and how subjectivity affects the perceived hazard.

Categorization of Signal Words

Figure 5.4 summarizes the categorization of words. Half of the participants believed that *protect* was considered most safe (n=14, 64%) while *hack* was unanimously considered most dangerous (n=22). Aside from *protect*, *online* and *message*, adults

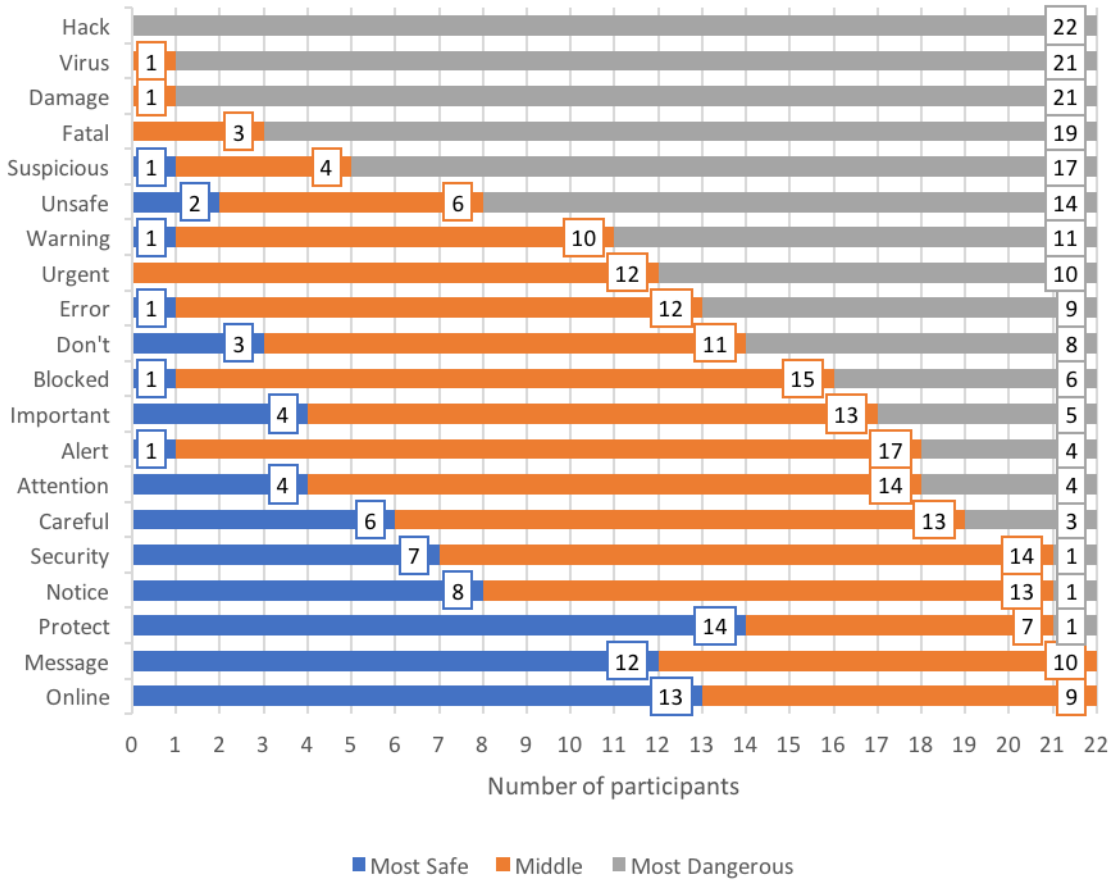


Figure 5.4: Number of adults placing words in each severity category.

were more likely to categorize these signal words in the middle or dangerous categories.

Adults found words to be easiest to categorize out of the three parameters (n=13, 59%). However, some adults had difficulty placing words because of the lack of context or explanation relating to the words, multiple words that are similar to one another, different implications of a word, and uncommon words for warning messages.

5.2.2 Card Ranking

Participants ranked the cards they had placed in each category in the order of most safe item to the most dangerous item. We present the results of the colour hazard ranking.

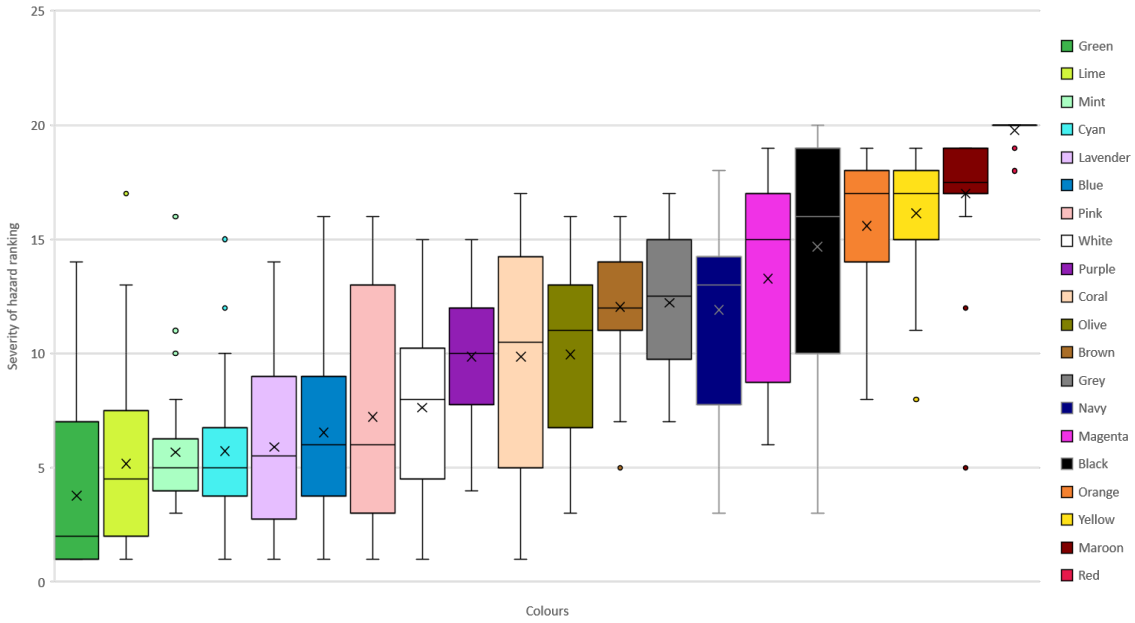


Figure 5.5: Adults' ranking of colours sorted by median rank, where rank 1=most safe and 20=most dangerous.

Hazard Ranking of Signal Colours

Figure 5.5 summarizes the colour hazard ranking. Participants found *green* to be safest while *red* was considered the most dangerous. Similar to children, adults had a high level of agreement for ranking the colour *red* as the most dangerous (rk=20, m=20). Others (e.g., *pink*, *coral*, *magenta* and *black*) had high variability in their hazard ranking.

Hazard Ranking of Signal Symbols

Figure 5.6 represents the symbol hazard ranking. Adults agreed on the ranking of *happy face* (rk=1, m=1) as the most safe and *skull and crossbones* (rk=20, m=20) as most dangerous symbol. Symbols such as the *police officer/security guard* and *stop hand* had the most variability.

Hazard Ranking of Signal Words

Figure 5.7 illustrates the word hazard ranking. Adults agreed that *online* was the safest (rk=1, m=2) The words *damage* (rk=17, m=17), *hack* (rk=18, m=18), *virus*

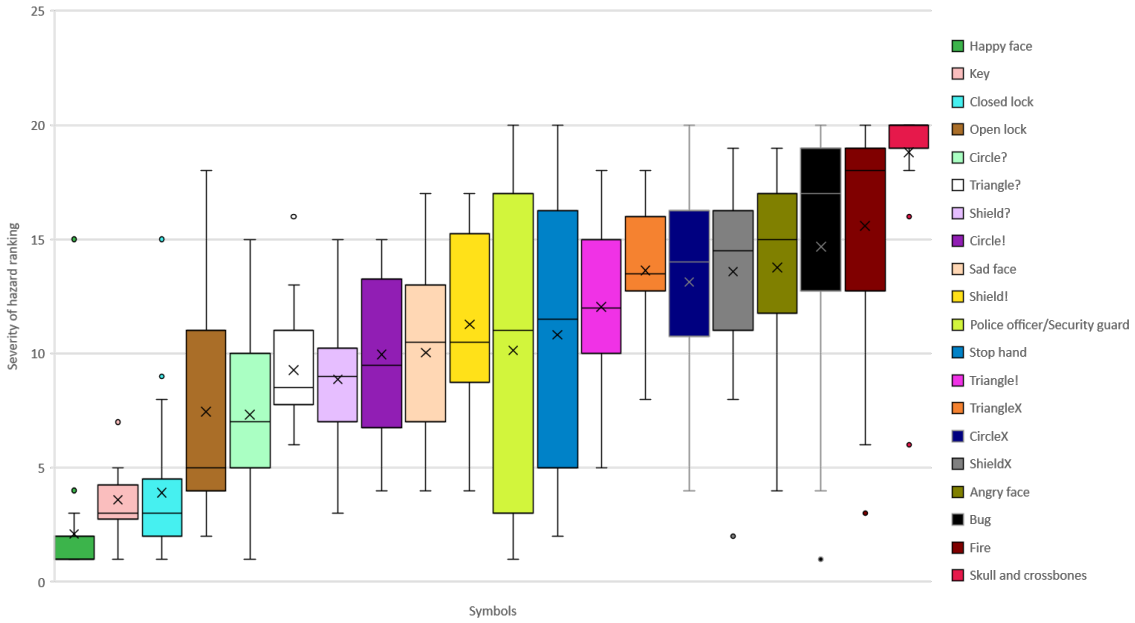


Figure 5.6: Adults' ranking of symbols sorted by median rank, where rank 1=most safe and 20=most dangerous.

(rk=19, m=18) and *fatal* (rk=20, m=20) were most dangerous. Word such as *security* had the most variability.

5.2.3 Qualitative Themes from Card Categorization and Ranking

Participants' comments during the categorizing and ranking activities were recorded and transcribed. Figure 5.8 represents adults' most frequently used terms when describing colours, symbols and words. The participants most often used terms such as "dangerous", "colour", "safeness", and "warnings".

We extracted a total of 1038 excerpts for colours, 762 for symbols and 708 for words. Themes are not mutually exclusive and therefore, one excerpt may be coded under multiple themes.

Signal Colour Themes

Figure 5.9 summarizes the distribution of the excerpts for colours. The most discussed colours were *red*, *black*, and *yellow* and *orange*.

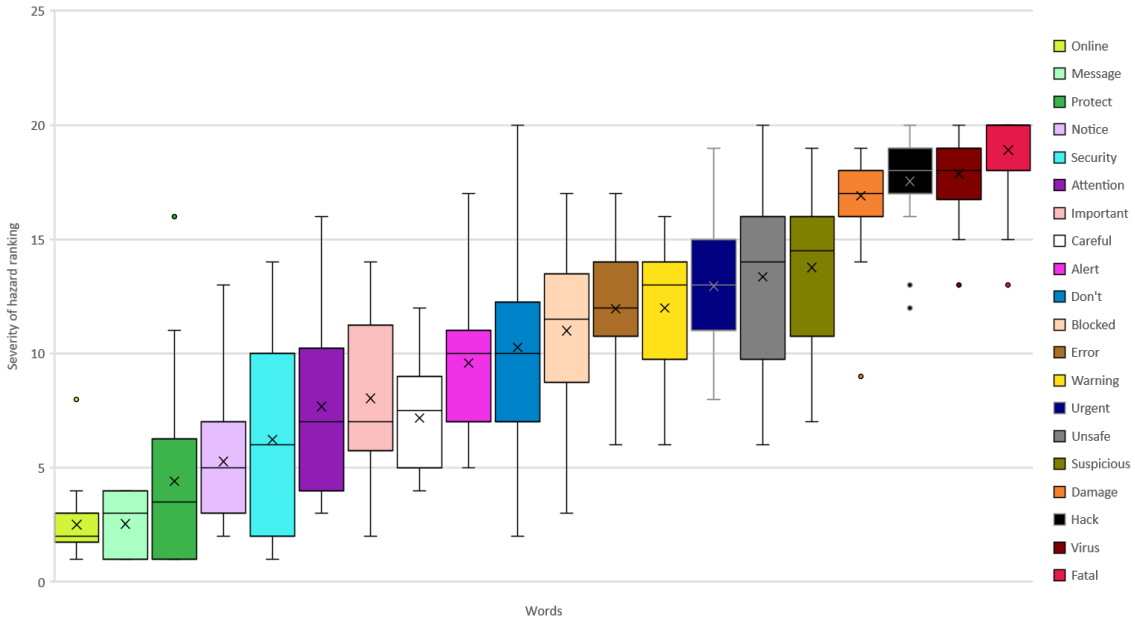


Figure 5.7: Adults' ranking of words sorted by median rank, where rank 1=most safe and 20=most dangerous.

Red was coded under *subjective perception* (*ne*=n excerpts=17), in which the participants regarded the colour to be negative (*ne*=7), attention grabbing (*ne*=6) and common (*ne*=3). Participants described *red* using *contextual associations* (*ne*=33) with road signs and lights (*ne*=14), social conventions (*ne*=5), nature (*ne*=5), technology (*ne*=4) and media (*ne*=4):

> "Most vibrant red, which means it's the least safe. The association is with experience, red usually needs your attention. So with traffic for example, with a stop sign, even blood in scary movies. Anything that's either scary or dangerous or just needs your attention." **A01**

> "Red is always in every kind of cultures, in traffic signs, it is a sign of danger, so that's gotta be the first choice [for most dangerous colour]." **A15**

Black was discussed using *contextual associations* (*ne*=16) with technology (*ne*=9), nature (*ne*=4) and social conventions (*ne*=2):

Figure 5.8: Word cloud to visualize adults' most frequently used terms when describing colours, symbols and words.

> "[Black] reminds of the abyss, nothing. I am agnostic so once you die, it will be all black. We're conditioned to think that, it could be all white for all we know, but when you see pictures of space, it's black. You are much more aware at night. With computers when you get black screen, a blue screen is worse but black is just empty, there's nothing." **A03**

> "Let's say you get a virus. You are trying to start up your computer, there is no response on the monitor. You see black. Black hole. Another death related kind of colour." **A13**

Participants considered the colour *yellow* to be *associated with other parameters* (ne=2), such as the word "warning". *Yellow* was also directly associated with the level

Colour themes	Ambiguous	Association with colours/hues	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Black	6	11	1	2	8	16	15	59
Blue	1	16	1		10	11	12	51
Brown	8	11	1		7	5	9	41
Coral	9	11		1	4	5	4	34
Cyan		23		1	11	16	13	64
Green	1	4		3	11	24	14	57
Grey	12	11		2	5	10	9	49
Lavender	2	23			5	12	9	51
Lime	2	21			6	7	7	43
Magenta	1	27			7	5	10	50
Maroon	3	30			6	3	8	50
Mint	2	19			4	8	14	47
Navy	1	29	1	1	6	7	6	51
Olive	3	19	1		6	12	8	49
Orange	1	20	1		5	18	13	58
Pink	2	20			6	14	7	49
Purple	1	21		1	9	10	11	53
Red		7	1	2	11	33	17	71
White	17	5			8	13	10	53
Yellow	1	11	2	1	15	18	10	58
Total	73	339	9	14	150	247	206	1038

Figure 5.9: Number of excerpts per theme for colours. Orange = Most frequent theme per colour, □ = Most frequent colour per theme.

of danger (*ne*=15). It was mostly seen as a dangerous (ne=7) or potentially dangerous colour (ne=7). *Yellow* was described using *contextual associations* (*ne*=18) to road signs and lights (*ne*=12), technology (*ne*=2) and nature (*ne*=2):

> "If I am driving, with red you know you have to stop, but if I hit a yellow light, it's like do I stop or not, do I accelerate or brake?" **A03**

> "[Yellow means] danger. In traffic signs, if you don't slow down, you are going to have an accident but it is not stop completely. You have a bit of opportunity to go through. As far as cybersecurity, the first thing I think of is on Mac, you can close the screen. It minimizes. [On the other]

> extreme, you have green to blow it up and maximize [the] window, red to close and yellow [to] minimize. I couldn't tell you what it does if I didn't have a Mac though, so it has a dangerous connotation. [Like] slipping on a banana peel." **A13**

Adults considered *orange* to be closely *associated with other colours and hues* (*ne*=20), most referred to similarities with other colours (*ne*=6):

> "[Orange is] similar along the lines of red and maroon, but [with] just a slight less degree of immediacy. A little bit of 'proceed with caution' rather than 'stop' to me. [Orange is a] bright colour that catches your eye and makes you stop because there could be a threat." **A17**

> "[Orange is a] bright colour in contrast to blue." **A21**

Most colours had some excerpts falling under the *association with colours and hues* theme (*ne*=339) because participants often discussed similarities with other colours (*ne*=176), associated dark colours together (*ne*=50) and contrasted differences with other colours (*ne*=30). For example, *maroon* (*ne*=14) reminded participants of "red", "magenta", "black", "brown" and "olive". *Navy* was mostly associated with dark colours (*ne*=14) while *black* was considered different from other colours (*ne*=4).

Similar to children (Section 4.2.3), adults also believed that *white* was ambiguous (*ne*=17) because the colour appeared to be "neutral", "nothing" and "blank".

Signal Symbol Themes

Figure 5.10 summarizes the distribution of the excerpts for symbols. The most discussed symbols were *skull and crossbones*, *fire* and *bug*.

Participants discussed *skull and crossbones* (*ne*=23) with *contextual associations* related to warning labels (*ne*=12) and technology (*ne*=8):

> "I associate with poison, chemical labels from the lab, [it means] something has gone wrong." **A11**

Symbol themes	Ambiguous	Association with symbols	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Angry face	3	2	1		8	11	13	38
Bug	4	2	6	2	7	13	14	48
Circle!	2	5	3	1	5	5	6	27
Circle?	5	4	1		8	8	5	31
CircleX	2	1	3	2	4	12	10	34
Closed lock		6	2	2	7	11	6	34
Fire	1	1	1	1	10	19	16	49
Happy face					10	8	21	39
Key	2	7	2		15	8	3	37
Open lock	5	8		2	10	8	3	36
Police officer or Security guard	4	2	2		10	13	11	42
Sad face	3	2	2		10	12	15	44
Shield!	3	6	4		8	13	3	37
Shield?	7	3	1	1	8	13	2	35
ShieldX	3	3	2		7	9	9	33
Skull and crossbones	1	3	5		11	23	18	61
Stop hand		3			15	11	3	32
Triangle!	2	9	1	1	5	10	7	35
Triangle?	8	3		1	8	13	2	35
TriangleX	3	3			7	13	9	35
Total	58	73	36	13	173	233	176	762

Figure 5.10: Number of excerpts per theme for symbols. Orange = Most frequent theme per symbol, □ = Most frequent symbol per theme.

> "[Skull and crossbones is] a pirate symbol. I associate with bio lab and chemistry classrooms, [saying] don't use these chemicals. In terms of a computer, if that symbol pops up, I wouldn't think it would be a normal icon on [a] computer. It would [say you are] hacked or it would frighten people. It would usually show up on a website that is already dangerous itself. Just not good. I wouldn't want this symbol to show [up] to say, 'Hey, something is wrong with your password'. My computer would be more frightening." **A12**

Fire was discussed using *contextual associations* (*ne*=19) with technology (*ne*=13) and warning labels (*ne*=6):

> "[Fire is a] chemical symbol, [something] flammable. I don't know in terms of cybersecurity, but I associate fire with something bad." **A11**

> "[Fire is] something that is flammable, fire that can burn you. [It is a] WHMIS symbol for flammable. [Fire is] below skull and bugs because those two are more familiar to me on a computer. I have not seen fire before except for maybe on a firewall." **A17**

Just as children found *bug* to be *associated with other parameters*, some adults mentioned the word "virus" (*ne*=6). *Bug* was notably associated with *subjective perception* (*ne*=14), as it was seen as a predominantly negative symbol (*ne*=9):

> "I do not like creepy things, a worm or Trojan horse, another analogy to animals that I don't quite understand. I don't know how that can pop up and be positive." **A14**

> "I see [bug] as a virus with cybersecurity. Viruses are bad and dangerous." **A19**

All symbols had excerpts falling under *contextual associations* theme (*ne*=233) related to technology (*ne*=129), road signs and lights (*ne*=42), warning labels (*ne*=29), social conventions (*ne*=26) and media (*ne*=7).

Signal Word Themes

Figure 5.11 summarizes the distribution of excerpts for words. The most discussed words were *fatal*, *hack*, and *blocked* and *suspicious*.

Adults associated *fatal* with *subjective perception* (*ne*=20) and primarily considered it a negative word (*ne*=17):

> "Whether it be human or computers, for technology, [fatal] brings a very negative connotation." **A04**

Word Themes	Ambiguous	Association with words	Association with other parameters	From previous experience	Level of danger	Contextual associations	Subjective perception	Total
Alert	1	9	2	1	8	6	9	36
Attention	3	7	3		3	6	8	30
Blocked		1		4	9	14	12	40
Careful	1	4		1	13	5	5	29
Damage		4			4	15	12	35
Don't	3	1			9	7	7	27
Error	1	4	1	2	4	11	14	37
Fatal	1	1	2	3	6	14	20	47
Hack	1	4		1	3	18	14	41
Important	1	8	1		5	8	8	31
Message	5	1			8	11	5	30
Notice	4	11		1	7	8	3	34
Online	2		1		10	16	3	32
Protect	1	6		1	6	13	2	29
Security	3	5			7	16	6	37
Suspicious	6	5		2	11	11	5	40
Unsafe		7			12	11	9	39
Urgent		12	1		3	11	11	38
Virus		4		1	6	15	11	37
Warning		8	2	3	9	8	9	39
Total	33	102	13	20	143	224	173	708

Figure 5.11: Number of excerpts per theme for words. Orange = Most frequent theme per word, □ = Most frequent word per theme.

Hack was described using *contextual associations* (*ne*=18) to technology (*ne*=16):

> "[It is] commonly known that if you have been hacked, either your info [is] accessed by someone else or they can control your computer in some cases." **A20**

Blocked was discussed using *contextual associations* related to technology (*ne*=14), mostly influenced by participants' *previous experience* (*ne*=3):

> "My natural instinct when I see [the word block] on a site is that there's something wrong with the site's security, or the site's procedures. This

> doesn't mean I'm not going to go onto it. You have blocked content all the time and you can bypass it. It is more cautionary for sure, though." **A04**

Suspicious was considered ambiguous and "unclear" (*ne*=6) compared to other words. Some excerpts relating to *suspicious* were coded under the *level of danger* theme (*ne*=11) and the word was predominantly considered "potentially dangerous" (*ne*=6). It was also described using *contextual associations* (*ne*=11) with technology (*ne*=10):

> "[Suspicious is] likely to be something that could be dangerous. Something that is detected as could be, most likely isn't. Should tread with caution and again, similar to unsafe, if you turn around or close that ad or change the course of action, you won't be damaged. It's a little bit of warning message." **A17**

> "[Suspicious] would be a cause of concern, but it doesn't mean there is something necessarily wrong if you know what you are doing. Downloading something from a website or using a software or trying to open a file [on] your computer that you know is safe but the computer thinks is suspicious. Since you know it's safe, you can go ahead and open it anyway. I've seen this happen with my professors' PowerPoint presentations. They open it anyways because they know it's not serious." **A12**

Like colours and symbols, all the words had excerpts falling under the *contextual associations* theme (*ne*=224), such as technology (*ne*=209), social conventions (*ne*=12) and media (*ne*=3) subthemes.

5.3 Post-test Semi-structured Interview

Post-test excerpts were coded and organized by interview question. There may be multiple excerpts per participant and these may fall across different themes.

5.3.1 Definition of "Cybersecurity Warning Message"

Similar to children (Section 4.3.1), all adult participants gave reasonable definitions of warning messages based on HITL security communication types [13]. Predominantly, 20 participants defined cybersecurity warning messages as *warning dialogs*:

> "A message that comes from either server, browser, or possibly an anti-virus protection software on your device. It lets you know if anything malicious is on the device, like malware, spyware, viruses, worms." **A02**

> "An alert or message that will appear on your screen, potentially from an anti-virus software program, saying whether there are any issues, and if so, what they are, and trying to protect your computer and your information online and downloading and accessing the website." **A06**

Two participants believed that these messages were *notices* providing users information to make security conscious judgments:

> "A notification telling you that something they are going to do, or something that's happening to the machine that you're working on that's unsafe, it needs your attention. It's asking you to be cautions and read through the information so that you can get the information you need to make your decision." **A04**

> "It should be if the system is working correctly, something preemptive, that notifies you that an action you make in the future could cause damage to your software and/or hardware. It shouldn't come after something bad happens, [it should come] before something bad happens. That's more of when the anti-virus comes in." **A07**

5.3.2 Attitude Towards Cybersecurity Warning Messages

Thirteen participants believed that warnings were *both* positive and negative. Warnings were considered *positive* when they alert users of a threat, allow users to recognize

threat, help users take action to remove or mitigate threat, explain the risks and consequences, confirm the safety of the activity or protect users' devices and information. Conversely, warnings were seen as *negative* when they are fake, phishing messages, give viruses, interrupt users' activity, scare and overwhelm users or when users become desensitized to the messages after repeated exposure. The following are some of the adults' comments:

> "Both, I want to see [warnings] if something is concerning on a website or app, I want notifications, but it is also negative. It makes me feel like something has been compromised and I should be cautious when proceeding." **A04**

> "Both - there can be phishing ones. It depends on context. If I really want to do something and I know it's a safe site but my security thing comes up and it won't let me, or [if] I am familiar with the site, then it will be annoying. If it is dangerous/serious ones, then I will take it. It is better to have [warnings] then not." **A09**

> "Both - the goal of these messages is more of a positive one, positive in what they are trying to get you to do. To stop and look into it and take action. What is annoying is when the messages come up and you are not sure what they are trying to tell you, very vague, like 'error error'. If they are more specific in what they are trying to do, then you are more likely to action, like 'Error, this website is unsafe'. But if it's just 'error' and theres nothing attached to it, then it's not very convincing." **A11**

> "Both. If it is from a legitimate source, like person from the bank, or email accounts that is telling you don't click on this certain phishing link, then that is a good thing. Protect your email accounts. Bad because we have been desensitized to it, because it's just a bunch of pop-ups that are nonsense, most are fake. They say you have a virus but you really don't, and you'll only get one if you click on them and follow their directions." **A17**

Six participants found warning messages to be exclusively *positive*:

> "It has to be positive. These messages will prevent any further problems that you will have. I don't see anything negative of that." **A15**

> "Positive. Generally speaking, it is a protective mechanism, keeps you from ruining your device. You can restrict violent or negative imagery for children. It is not positive as in happy but beneficial." **A20**

On the other hand, two participants believed warnings to be only *negative*:

> "Negative. I think of it as someone advertising as something. You normally have a cyber-safety net on your computer, so if you can't go further, then you shouldn't go further. If I see a cybersecurity message, I take it as someone trying to sell me something or that they have virus in it and are trying to provoke you into clicking on it. Double negative." **A05**

> "Negative, if it is secure, then it wouldn't show you messages. If nothing is wrong, it wouldn't tell you anything." **A16**

Like children, adults viewing warnings as negative misunderstood the purpose of warnings and associated them with malicious intentions.

5.3.3 Type of Cybersecurity Warning Messages

Adults were also asked to share a story about their previous experiences with cybersecurity warning messages.

Prior to receiving warnings, adults were generally browsing the web, downloading files, streaming videos, using online banking or social media. Thirteen participants encountered *pop-ups* during an activity:

> "When Facebook was caught with the information leak, as soon as you logged on, there was a pop-up on Facebook that took up your [whole] screen. It was saying, 'We are sorry this happened, you should change your password, change this and that'. Twitter sent an email as well as

> a pop-up, all info was compromised for all their users, so they asked all their users to change their passwords because all the passwords were in plain text." **A12**

Seven participants encountered *system status* indicators that they interpreted as a security warning:

> "I don't have much space on my hard drive, uploading tons of photos, my computer stopped because there wasn't space on my hard drive. I got a message saying uploading stopped because you only have 2.8 GB left on your hard drive. There was no corrective action I was told to take." **A21**

Five participants experienced *phishing* messages:

> "I was browsing, as per usual, this Mac keeper pop-up came. It had a timer with x amount of time on it, saying if you don't download the app before the time runs out, you'd lose all your info. This happens about once a week and has been happening over many years so I just ignore it. It was specific to my MacBook Pro. They are not real security warnings - malware. I never see it on a tablet." **A13**

Five adults believed that the warnings provided *actionable advice* such as instructions on how to deal with hazardous situations:

> "I remember trying to access a website, I think it said, 'attention' and all red and the page was red. It was telling me something is unsafe, and to go back to the previous page and get off the website. A little rectangle on the web page, not the whole screen. I left the website. Went back." **A19**

Five participants came across *viruses* disguised as warning messages and two messages turned out to be *ads*:

> "The first time it happened, I clicked on it and I got a virus. I was in trouble at work, [my colleagues] made fun of me, but I wasn't the only one. That was my big learning curve. An email came through, I clicked on it thinking it was [an] inquiry from an international student, it ended up being a virus." **A05**

> "I was watching movies, you clicked a movie and this page is loading, it will load a separate page with ads, sometime there's a sound associated with it. That happened in class one time. I just closed it. Sometimes you see something and panic, you don't even look at it and quickly close it." **A16**

5.3.4 Reactions to Cybersecurity Warning Messages

Adults (n=17) reported that they mostly *read* the messages, but more than half (n=13) reported that they *continued with the activity by avoiding* the warnings. They did so by ignoring the message, dismissing, closing or exiting the pop-up window, tab or the website:

> "I read it usually. If it is something I have seen it a few times, I might gloss over it, I won't read it carefully. If it has very significant impact on my life, like with banking, I will read it more thoroughly." **A04**

> "I just leave, I [click to] go back. I see the one word that says attention and then I [click to] go back. I think I close it. I leave." **A19**

After encountering the warnings, three participants exited the warning and *stopped the activity* all together:

> "I don't look at them at all, I exit. I close them. I do something else." **A08**

Two participants mentioned that they *received help*, two *turned off and restarted the device*, two *continued with the activity after interacting* with the warning message and two *ran a malware scanner*:

> "...if you are at work or school, the computers have a lot of sensitive information so if something is wrong, I always go to the manager, someone who has been around for a long time and wait for permission." **A02**

> "I try to refer to my experience with computers/devices when dealing with these messages. Usually I know what to do, most of the time. And if I don't know what to do, just turn it off, give it a break, start it up again, unless it's something really serious." **A02**

> "More likely to click on it if it's okay and I'm familiar with the website." **A06**

> "If I know it's my security thing on the message, if it has McAfee or a brand on the warning message, I will read it. I will become familiar with it. I will read it if it is the company I am currently with. If it is random things, like, 'we just scanned your computer and found 50 viruses', I am not paying them, so there's no reason for them to be scanning it. I will ignore and close them. If it's the one I'm paying for, I would go to the desktop native app and scan from there because I am paying for it, I know it's legitimate. The pop up might be fake, but I would definitely go to my native app and do the scan." **A09**

5.3.5 Reporting Habits for Cybersecurity Warning Messages

Half of the adults (n=12) mentioned that they *did not report to anyone* after encountering warnings because they either already knew what the messages meant and how to deal with them, or they would search on Google to figure out what to do.

However, some adults mentioned that they told *family* (n=9) members that have more experience with technology and *friends* (n=4), and some received *professional help* (n=4) from the IT support, the Apple store, and colleagues:

> "I consider myself as relatively tech-savvy and I deal with it. My mom does show me stuff though." **A01**

Those that did not report to anyone mentioned that others came to them for help instead:

> "[I show warnings to my] parents [to let them know] messages like these are 'normal'. My high school teachers got me to help them with computers, to look at them, tell them what they mean. I deal with it mostly." **A12**

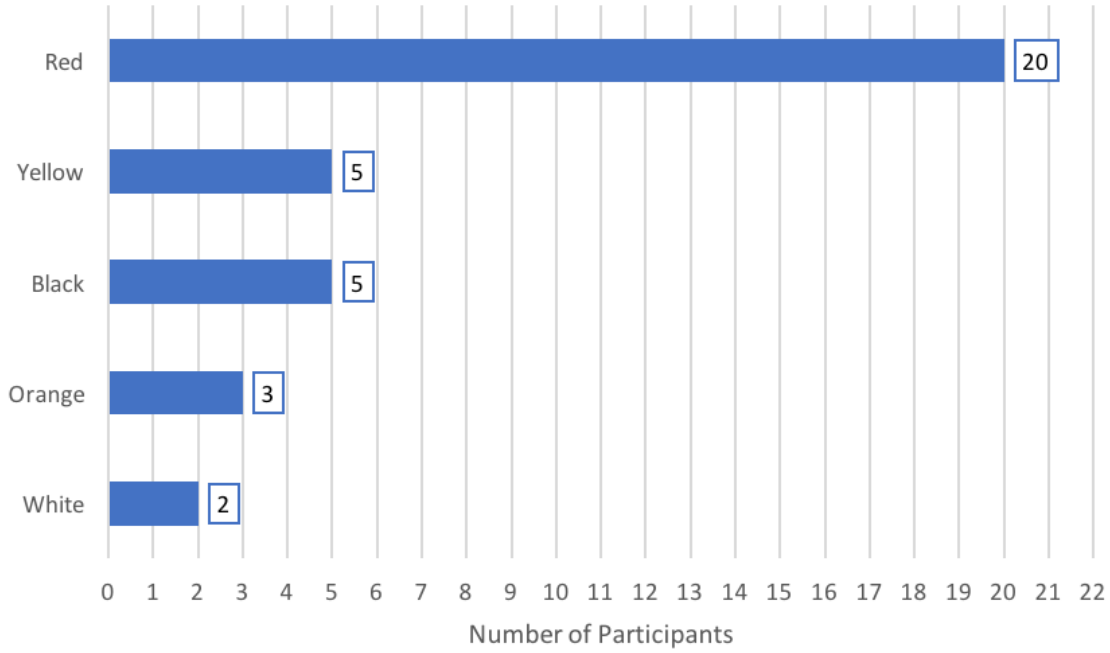


Figure 5.12: Adults' expectations for cybersecurity warning messages for colours.

5.3.6 Adults' Expectations for Cybersecurity Warning Messages

Participants gave suggestions on warning design parameters and other characteristics that they would expect to find on warnings to indicate something dangerous happening.

Colours

Figure 5.12 summarizes adults' expectations for colours that should be used on warnings to indicate a severe hazard. Similar to children (Section 4.3.6), most adults (n=20) expected to see *red* above all other colours:

> "First thing you respond to are colours. Colour is important. You said [the warning message] is very dangerous, so the most dangerous colour [should be used] - red." **A03**

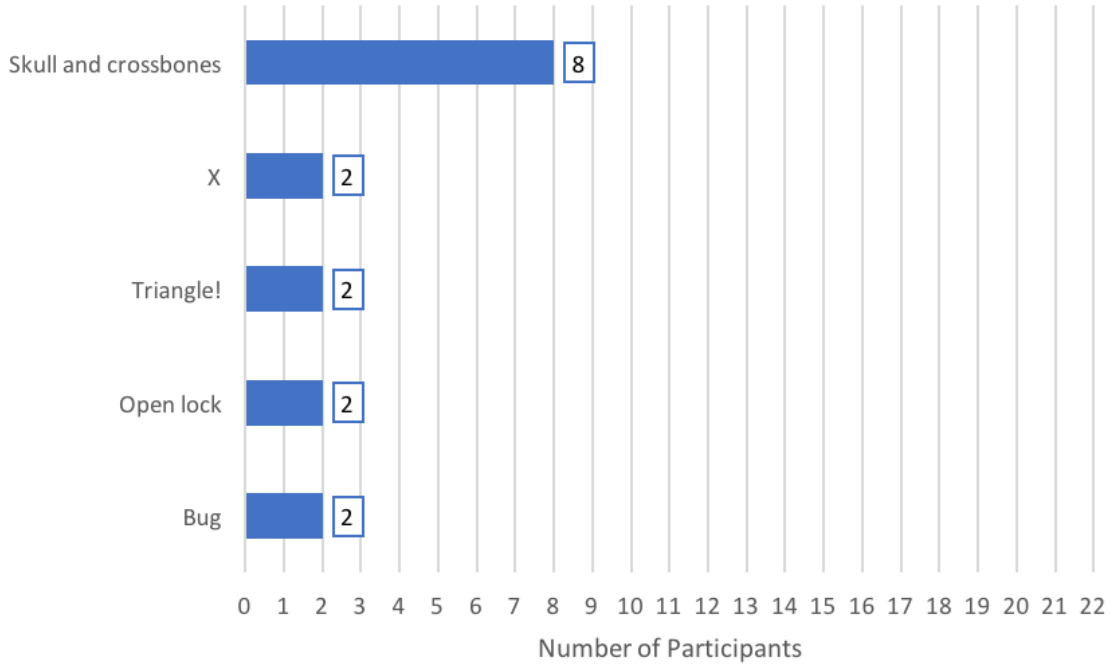


Figure 5.13: Adults' expectations for cybersecurity warning messages for symbols, sorted by most prevalent to least prevalent.

Symbols

There was less agreement for symbols, as depicted in Figure 5.13. Eight participants expected to find *skull and crossbones* on dangerous warning messages.

Two participants suggested symbols such as an "octagon with stop sign" (**A02**) and "something from the middle category" (**A03**). Participant **A03** explains his rationale: "You want [a symbol] that doesn't [make you] feel like you are being attacked personally. You want something that tells you that it means well for you. It's on a fine line, [like] something in the middle."

Words

Figure 5.14 illustrates adults' expectations for words. There was variability among the participants on the word they expected to see to indicate something dangerous. Aside from the 20 signal words used for categorization and ranking, one participant suggested the word "restricted" (**A04**).

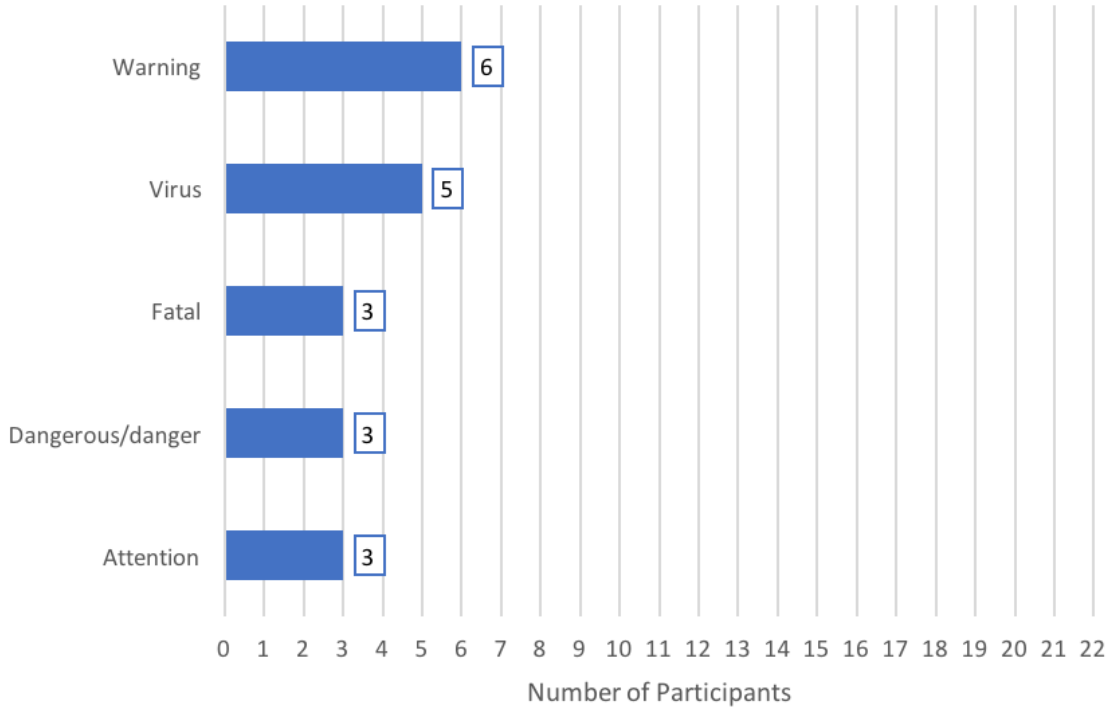


Figure 5.14: Adults' expectations for words
Adults' expectations for cybersecurity warning messages for words.

Other Characteristics

Adults provided further suggestions for effective warning messages. We identified seven trends that were consistent with the children's interviews, as well as two additional trends summarized in Figure 5.15.

Adults mentioned that risk communication was fundamental in warning messages and that they should provide *explanation of the risk* (n=9):

> "What if a poor beginner stumbles upon an error code, not everyone is [an] engineer out here. Translate errors and codes to plain English, not everyone can understand the computer hardware/internet lexicon or jargon." **A02**

> "Words are last thing you are paying attention to. But if you're actually reading, you don't want just a word, you want an explanation. If you are

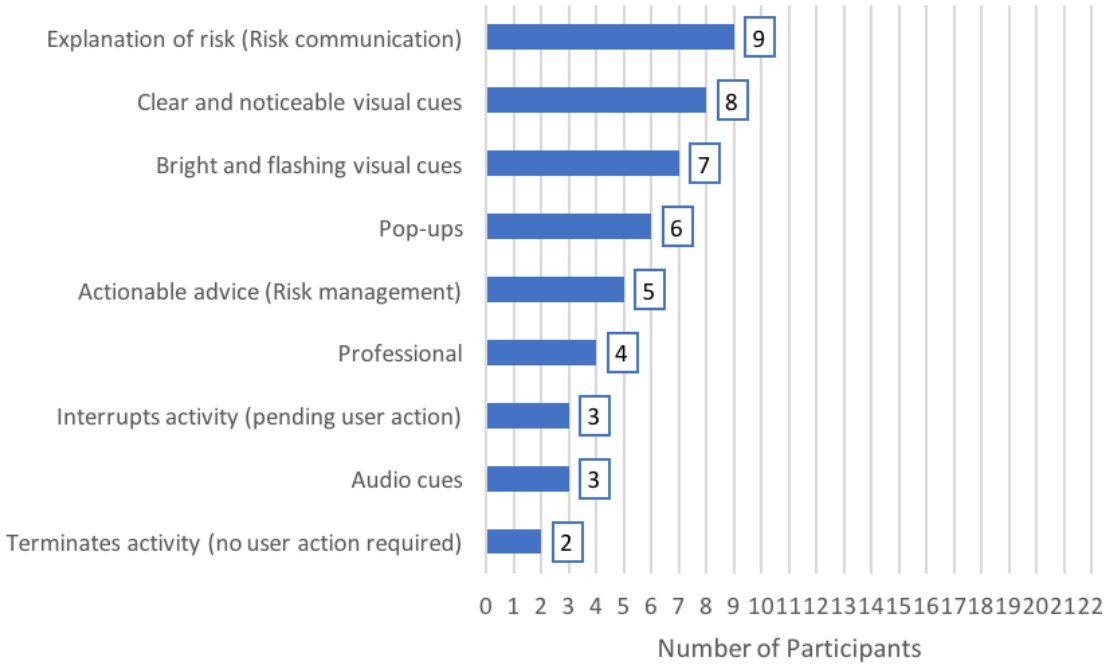


Figure 5.15: Adults' expectations for cybersecurity warning messages for other characteristics.

> reading, that means you didn't catch the hint with the colour or with the symbol, so you want a full explanation." **A03**

> "I want it to expand and explain what exactly the breach and security message is. In layman's terms and not in jargon." **A13**

> "Explicitly say what it is, not just codes like Error 777, no technical jargon, because I don't know what that means. Should say exactly [where] it is coming from. Click for additional information. Says exactly what the problem is, where it's coming from, all the information so that I don't take it lightly." **A18**

Adults also highlighted the importance of visual cues to capture users' attention. They suggest *clear and noticeable* (n=*8*) and *bright and flashing* (*n*=7) messages:

> "Clear message but not too many words. Big font, not too many small words, making sure that it's clear when you read the message." **A17**

> "I would go for bold colours and big writing. You don't really read the small writing." **A19**

> "It still should be slightly bright to grab your attention. Reds, yellows, but not too many because it becomes overwhelming and flashy." **A17**

> "I'm really just thinking of road signs, a railway crossing says, 'don't cross', and they're really taking precautions to make sure no one crosses, there's a light flashing." **A18**

Some participants proposed that warnings should be *pop-ups* (n=6), while others suggested including more information concerning risk management like providing *actionable advice* (n=5):

> "I want it to give me a red pop-up with big sign and explanation at the top. I also want some explanation of why it happened underneath the sign so that I would understand it is dangerous." **A10**

> "Say what the repercussions can be, and what I can do. If my files are corrupted, what do I do with it, is there a way to go back cause I don't necessarily know what that means. [I also want] a link [that says] 'click here for more information'." **A18**

Some adults emphasized the importance of interrupting the user to ensure that they pay attention to the warnings. Participants suggested *activity interruptions pending user action* (n=3) and *audio cues* (n=3):

> "Some sort of way that it's kind of in your computer, like only your computer can show you that. [Does] not necessarily [have to be] on the page, it [should] block you from accessing other things on [the] computer until you deal with it." **A18**

> "I actually want audio sound. Something that talks and plays recordings [like], 'Warning, there is a breach happening'. You hear some of them [in warnings] but not usually. [Generally,] if it is audio, it doesn't expand on it. It says, 'warning' and that's it." **A13**

Adults hoped to see security warnings that are *professional* (n=4), and can *terminate the problematic activity with no required user action* (n=2):

> "[Warnings that] look professional, look like it's from a reputable source. It needs to be labelled from Apple Macintosh or Windows logo." **A17**

> "If it's that serious, then just shut the problematic tab down itself." **A09**

5.4 Summary

We gathered adults' perceptions of warning design parameters and their expectations for warnings that indicate danger. The results of this study with adults are consistent with the literature on warning design parameters [3,16,25–28,36,39,64] and are similar to the findings from our study with children. Adults' ranking of signal items for dangerous and safe warning messages were fairly similar to that of children. Adults considered *red*, *skull and crossbones* and *fatal* to be most dangerous, while *green*, *happy face* and *online* were safest. Adults determined the severity of hazards based on associations with other concepts and experiences. Adults' expectations for dangerous warning messages were fairly consistent with the items deemed dangerous during their activity: *red*, *skull and crossbones* and *warning*. They also highlighted the importance of clear *risk communication*. We compare and contrast the results from both studies, and discuss secondary findings in the following chapter.

Chapter 6

A Comparison of User Studies

Two studies were performed, first with children aged 10 to 12 years old and then with adults between the ages of 18 to 51. Our results indicate some differences between children and adults on their perceptions of, previous experiences with, and expectations for, cybersecurity warning messages. The groups had similar notions about which signal colours, symbols, and words indicate most dangerous and safe situations. They expressed similar concepts that shaped their risk perceptions of warnings. We did not observe a huge gap between children and adults' previous experience with warnings. In this chapter, we compare our results from both studies.

6.1 Hazard Ranking Comparison

As summarized in Figure 6.1, children and adults had fairly similar median rankings for the top 3 most dangerous and safest signal colours, symbols and words. Dark green boxes represent complete match in rank (e.g., both user groups ranked *red* as the most dangerous colour), and light green boxes represent a partial match (e.g., both groups placed *maroon* in the top 3, but adults ranked *maroon* as the second most dangerous while children ranked it as the third).

Both groups considered *red*, *skull and crossbones* and *fatal* as the most dangerous, and *green* and *happy face* as the safest. In comparison to adults who determined *online* as the safest word, children placed it as the third, and *protect* was ranked the safest instead.

As depicted in Figure 6.2, both groups had most to say about similar colours, symbols and words, and generally used similar reasoning to determine their perceived severity.

		Children	Adults
Signal Colours	Top 3 most dangerous	Red	Red
		Black	Maroon
		Maroon	Yellow
	Top 3 safest	Green	Green
		Cyan	Lime
		Lime	Mint
Signal Symbols	Top 3 most dangerous	Skull and crossbones	Skull and crossbones
		Bug	Fire
		Fire	Bug
	Top 3 safest	Happy face	Happy face
		Closed lock	Key
		Police officer/Security guard	Closed lock
Signal Words	Top 3 most dangerous	Fatal	Fatal
		Hack	Virus
		Virus	Hack
	Top 3 safest	Protect	Online
		Security	Message
		Online	Protect

Figure 6.1: Comparison of children and adults' top 3 rankings for most dangerous and safest signal colours, symbols and words. Dark green = Complete match in rank, Light green = Partial match.

6.1.1 Warning Signal Colours

Overall, we observed several trends for colours. 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 on colours and their levels of risk in the context of warnings [25, 28, 36].

Children and adults showed a high level of agreement on the hazard ranking of *red*. Several participants in both groups explicitly mentioned that *red* was "bad" and *green* was "good" (n=5 children, 6 adults), which could suggest that this concept may have been ingrained early in young children 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 playing games such as *Red Light, Green Light* [56]. In this game, a person acting as a stoplight gives clear red or green

		Children	Adults
Signal Colours	Most discussed colours	Black	Red
		Red	Black
		Green, White	Yellow, Orange
	Most discussed colour themes	Association with colours/hues	Association with colours/hues
		Contextual association	Contextual association
		Level of danger	Subjective perception
Signal Symbols	Most discussed symbols	Skull and crossbones	Skull and crossbones
		Police officer/Security guard	Fire
		Bug, Angry face	Bug
	Most discussed symbol themes	Contextual association	Contextual association
		Subjective perception	Subjective perception
		Level of danger	Level of danger
Signal Words	Most discussed words	Online	Fatal
		Blocked	Hack
		Fatal	Blocked, Suspicious
	Most discussed word themes	Contextual association	Contextual association
		Level of danger	Subjective perception
		Subjective perception	Level of danger

Figure 6.2: Comparison of children and adults' signal parameters and themes with the most excerpts. Dark green = Complete match, Light green = Partial match.

signals to represent stop and go, which may encourage children to form these colour associations.

Maroon was considered quite dangerous by both groups. Participants explained that the main reason behind *maroon*'s high ranking on the danger scale 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 colour but also middle/neutral together. It is showing danger but not as strong as red." **A10**

We found that participants' perceived level of hazard for colours was highly dependent on the each individual's subjective assessments. Colours with higher variability in their hazard ranking (e.g., *green*, *lime*, *white*, *blue*, *coral*, *olive*, *yellow*, *navy* and *orange*) also showed high variability in individuals' colour-emotion associations, personal preference and past experience with that colour [33]. In a study examining

college students' colour-emotion associations, Kaya and Epps [33] 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, [so] 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 colour, but if I had to rank it, it would be the least safe, in the middle." **A04**

Both children and adults found that it was more difficult to categorize colours than symbols and words. They emphasized that colour by itself did not give enough information to users to establish context for warnings. This finding suggests that colours may be more effective in communicating risk when they are presented in tandem with other design parameters. This is evident in the qualitative themes discovered from the participants' excerpts. Most participants associated colours (e.g., *black*, *red*) with symbols and words. For example, *red* was discussed using symbols like "fire", "stop sign" and "X", and words like "attention" and "urgent".

We also observed some differences between the two user groups. *Black* was considered one of the top 3 dangerous colours for children (rk=19) but not adults. Although *black* was still considered dangerous (rk=16), some adults said it was their "favourite colour" (**A08**) while children found it "scary" (**C21**). Research on colour-emotion associations show that children had negative reactions to *black* [6], but *black* elicited

both negative (e.g., depression, fear, anger) and positive (e.g., richness, wealth, power) responses in adults [33].

In our research, children considered *yellow* to be somewhere in the middle on the danger scale (rk=13) because even though it was a common colour seen on traffic signs and lights, *yellow* was also associated with the "sun" (**C10, C13**). This is consistent with the findings from a study that investigated children's emotional associations with colours, where they responded positively to bright colours like yellow [6]. In a general context, adults also associated *yellow* with positive emotions (e.g., happiness, excitement, sun, summer time) [33], but in the context of warning signs, they associated *yellow* with caution [25,36]. In our study, adults ranked yellow among the most dangerous (rk=18)

6.1.2 Warning Signal Symbols

Some trends were observed for symbols in both children and adults. 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 and crossbones, fire) were likely to be considered dangerous. On the other hand, symbols usually found on messages that indicate safety (e.g., happy face, closed lock, key) were considered safe. Both groups showed a high level of agreement on the hazard ranking of the two extremes, *happy face* and *skull and crossbones*, which suggests that these two symbols may be appropriate in communicating risk on cybersecurity warning messages.

Symbols that appear to have an "icon within an icon" were generally seen as ambiguous. Some examples include symbols that have combinations of outer icons *circle*, *shield* and *triangle*, with inner icons *?*, *!* and *X*. Children considered the symbol *circle?* to be the most ambiguous (ne=7), while *triangle?* was considered the most ambiguous for adults (ne=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**

> "[With triangle?, it 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. ? makes it ambiguous." **A07**

Both groups believed that symbols with X (e.g., *circleX*, *shieldX*, *triangleX*) were more dangerous than symbols with ! (e.g., *circle!*, *shield!*, *triangle!*) and symbols with ? (e.g., *circle?*, *shield?*, *triangle?*) were considered the safest.

When it came to symbols associated with emoticons like *angry face*, some adults believed that they were more effective for children. They believed that children would have easier time determining the level of hazard with emotive symbols because other symbols required more knowledge and experience:

> "[Is this] yelling or yawning? I'm gonna assume it's yelling, and that's a more negative [thing] 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 [they] have come across them in [the] media." **A20**

Contrary to their beliefs, both user groups had very similar rankings on *happy face* and *sad face*. Children and adults considered *happy face* to be safe (rk=1) and predominantly positive, and *sad face* to be placed somewhere in the middle category (rk=9). Interestingly, while adults considered *angry face* dangerous (rk=17), children ranked it in the middle (rk=11). Children had mixed opinions on where they categorized and ranked *angry face* because some children believed that these symbols were inappropriate on warnings. 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 websites won't use these faces (smiley, sad, angry faces). These are kind of funny, they won't use it to get anyone's attention." **C11**

We observed some differences in trends. Although both groups had mixed feelings on *police officer or security guard*, children considered it safe (rk=3) and generally 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 [an] imminent danger, or a possible threat." **A17**

Interestingly, while both groups associated the *closed lock* with safety, they had different opinions on the *open lock*. Given that a *closed lock* symbol in a web browser is a common security indicator [18], it would make sense for users to assume the opposite for the *open lock* symbol. However, adults found *open lock* to be safe (rk=4) compared to other symbols, while most children placed it in the middle and dangerous categories (rk=14). This finding may be due to the differences in the two groups' associations of *open lock* with physical security metaphors [52]. For example, the *open lock* may suggest that it is safe to proceed:

> "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 [means] something is opening. When you go into website, it could mean that you have access to it." **A09**

> "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 [symbol] in computer or cybersecurity [context]. 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 the doors or for their parents to unlock the locked screens on their tablets. When these children run into things that are unlocked without their parents' permission, it may insinuate that a stranger has access:

> "[When it is] unlocked, children can think they could go but it's not safe." **C10**

> "[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**

A few children categorized *open lock* as safe, interpreting the symbol as a safe indicator 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**

This suggests that the binary relationship could be easily misinterpreted when it comes to 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**

Children mentioned that symbols were the least difficult to categorize out of the three design parameters because they had previous experience seeing some of them:

"Symbols [are the] easiest. We see the symbols all the time, lock, I see in emails [and] bugs mean virus." **C01**

"[Symbols are] easy because I've seen most of the symbols here. It's easy for me to put it where it goes." **C11**

6.1.3 Warning Signal Words

Both groups agreed on the most dangerous words: *virus*, *hack* and *fatal*. Participants discussed the words *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 depended on their *subjective perceptions* to categorize and rank *fatal*, and they felt that the word predominantly had a negative

connotation associated with "death" (**C19-21, A2-3, A6**). This implies that when used on cybersecurity warnings, these three signal words may be highly effective in communicating high 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**

> "Something bad is blocked, yay." **A02**

On the other hand, being blocked could indicate how dangerous that website is:

> "[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 on words like *damage* and *suspicious* compared to the 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 children).

		Children	Adults
Previous experience	Online activities	Games	Social networking services
	Definition	Warning dialogs	Warning dialogs
	Perception	Both	Both
	Type of message	Pop-ups	Pop-ups
	Reaction	Get help, Read	Read
	Reporting habits	Adults	Do not report
Expectations	Top 3 colours dangerous	Red	Red
		Black, Yellow	Yellow
		White	Black
	Top 3 symbols dangerous	Skull and crossbones	Skull and crossbones
		X	X, Triangle!, Open lock, Bug
		Bug	TriangleX, Triangle, Key, Fire, CircleX, !
	Top 3 words dangerous	Fatal	Warning
		Hack	Virus
		Warning, Virus, Attention	Fatal, Dangerous/danger, Attention
	Top 3 other characteristics dangerous	Bright and flashing visual cues, Clear and noticeable visual cues	Explanation of risk (Risk communication)
		Explanation of risk (Risk communication)	Clear and noticeable visual cues
		Actionable advice (Risk management)	Bright and flashing visual cues

Figure 6.3: Comparison of children and adults' post-test semi-structured interview questions. Dark green = Complete match, Light green = Partial match.

6.2 Post-test Semi-structured Interview Comparison

The post-test semi-structured interview responses by children and adults are summarized in Figure 6.3.

Surprisingly, we did not observe a huge gap between children and adults' responses on their previous experience with warnings.

6.2.1 Online Activities

Both children and adults engaged in online activities mainly for entertainment purposes, as summarized in Figure 6.4. Children were much more likely to engage in *games* compared to adults, and as expected, did not engage in *professional or personal*

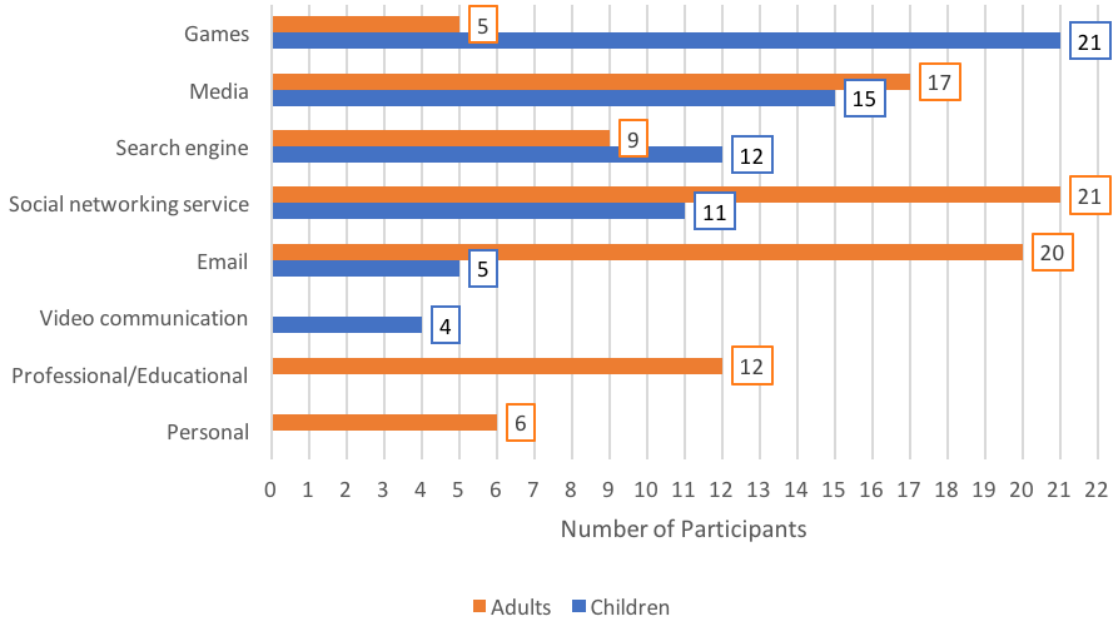


Figure 6.4: Comparison of children and adults' online activities.

activities such as online banking, travelling and shopping. Some children mentioned that they went online at school but did not specifically clarify for which activities.

6.2.2 Understanding and Attitude Towards Warning Messages

Using the definitions provided by Cranor [13] as a baseline, both user groups primarily understood warning messages to be *warning dialogs* (n=19 children, 20 adults). Adults also included *notices* within their description.

Both groups had similar attitudes toward cybersecurity warning messages, as shown in Figure 6.5. The majority of participants viewed warnings as *both* positive and negative. We found that those who viewed warnings *negatively* generally misunderstood the purpose of warnings and they 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.* [16], the general negative attitudes associated with warnings stemmed from users' negative past experiences, such as with messages that are annoying (e.g., interrupting users' activities).

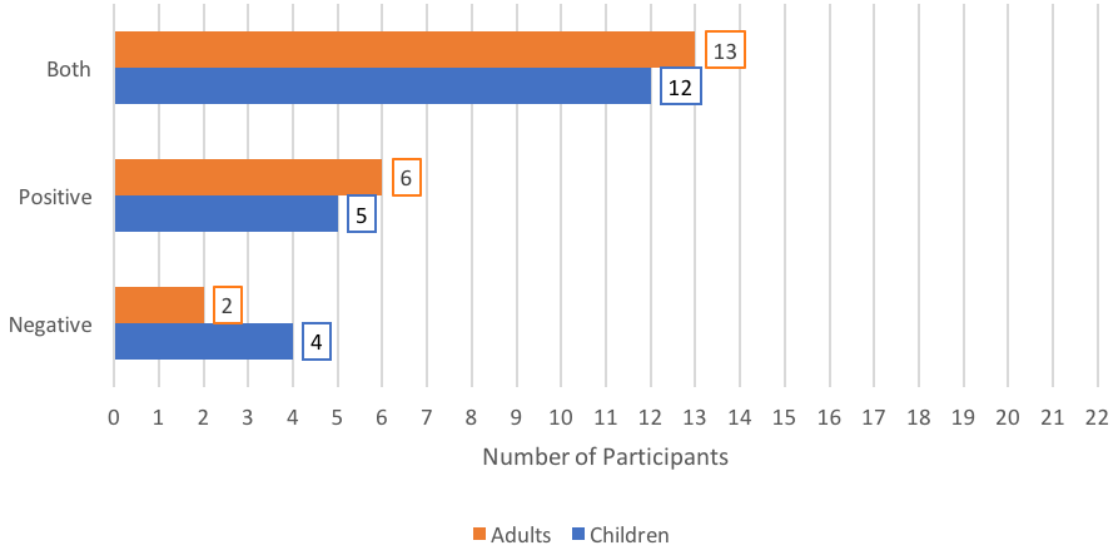


Figure 6.5: Comparison of children and adults' attitudes toward cybersecurity warning messages.

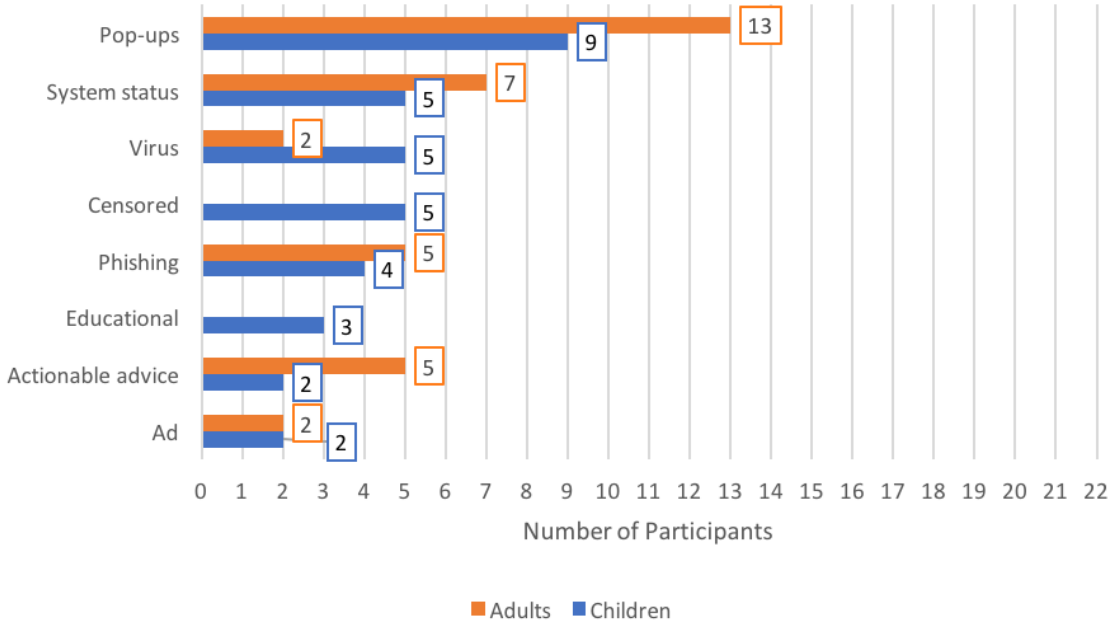


Figure 6.6: Comparison of children and adults' encounters with different types of cybersecurity warning messages.

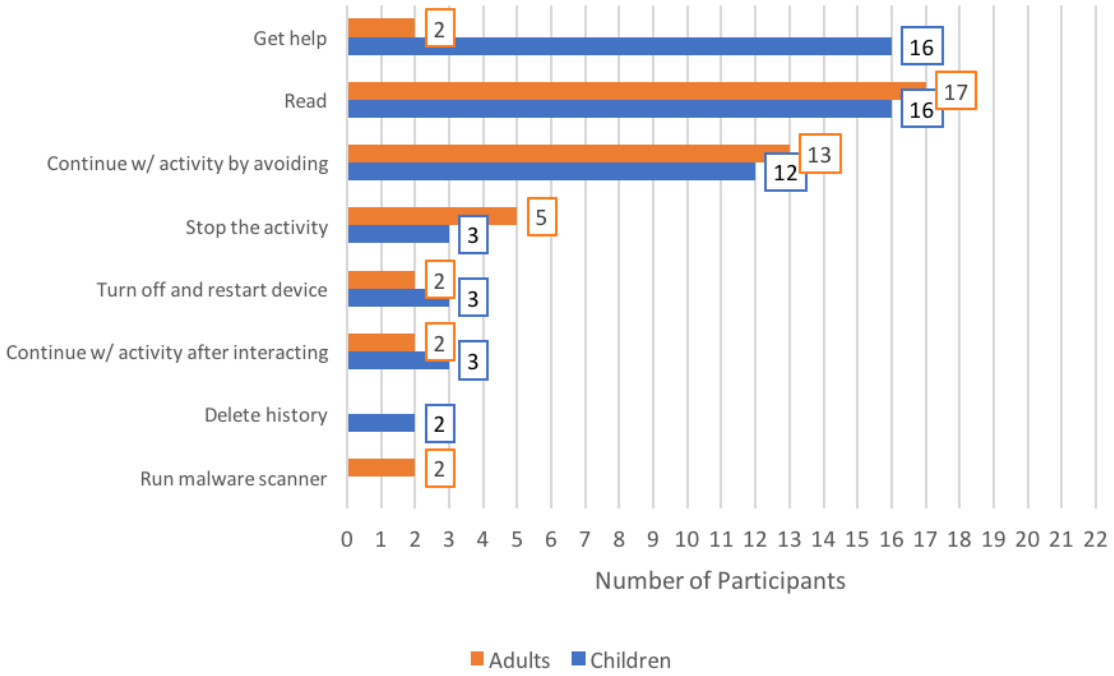


Figure 6.7: Comparison of children and adults' reactions to cybersecurity warning messages.

6.2.3 Types of Warnings

As depicted in Figure 6.6, both user groups mostly reported encountering *pop-ups* during online activities, followed by *system status* indicators that they interpreted as security warnings. Some children reported seeing *censored* content and *educational* messages, but these were not reported by any adults.

6.2.4 Reactions to Warnings

Most children and adults reported that they *read* the warning messages that they encountered, as summarized in Figure 6.7. Most children also *received help* from others, but the majority of adults did not. A significant portion of both groups reported that they try to ignore the warning and continue with their primary activity if possible. It also highlights that security is a secondary task [60] for both groups.

As summarized in Figure 6.8, most children reported that they showed cybersecurity warning messages to someone else while half of the adults *did not report*

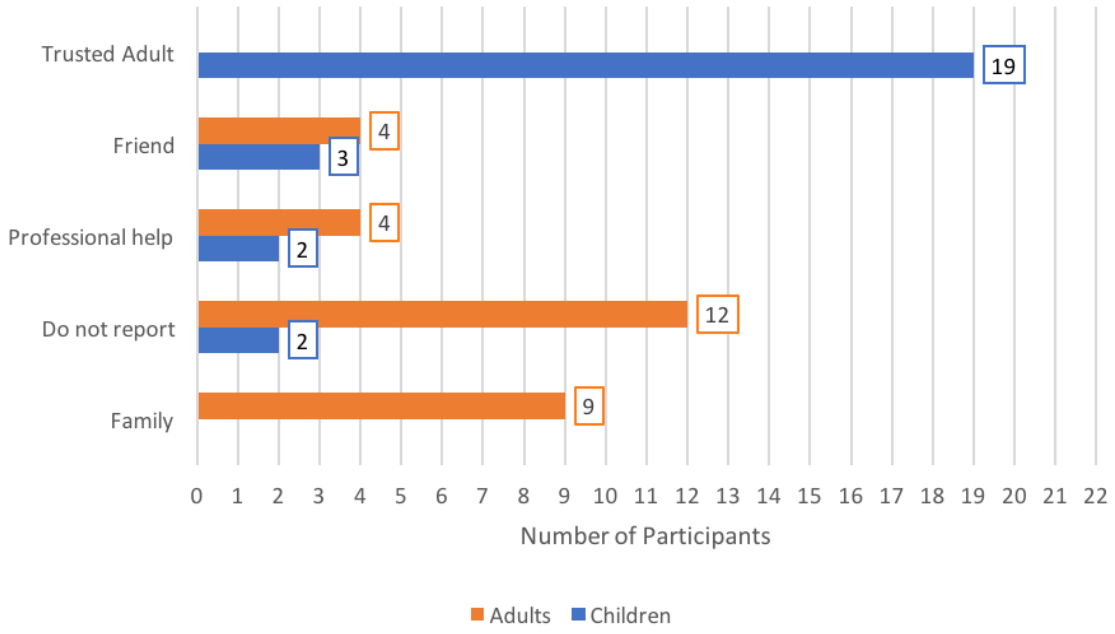


Figure 6.8: Comparison of who children and adults asked for help with cybersecurity warning messages.

to anyone. Children generally reported to *adults* (e.g., a parent, an older sibling, a teacher) rather than friends, and adults talked to someone more technology-savvy (e.g., *family* members, *friends*, *professional help*). Literature on children and online privacy found that children often depended on parents for advice and guidance [66,67]. Adults who did not report to anyone mentioned that they were confident in dealing with the warnings by themselves and that others came to them for help.

6.2.5 Expectations

Figures 6.9, 6.10 and 6.11 compare children and adults' expectations for signal colours, symbols and words on cybersecurity warnings that communicate danger. Both groups had fairly similar expectations. Children's expectations were consistent with their hazard ranking: *red*, *skull and crossbones* and *fatal* conveyed the most danger. Adults believed that *red*, *skull and crossbones* and *warning* conveyed the most danger.

Figure 6.12 summarizes additional suggestions for warning messages. Children highlighted the importance of other design characteristics that catch users' attention,

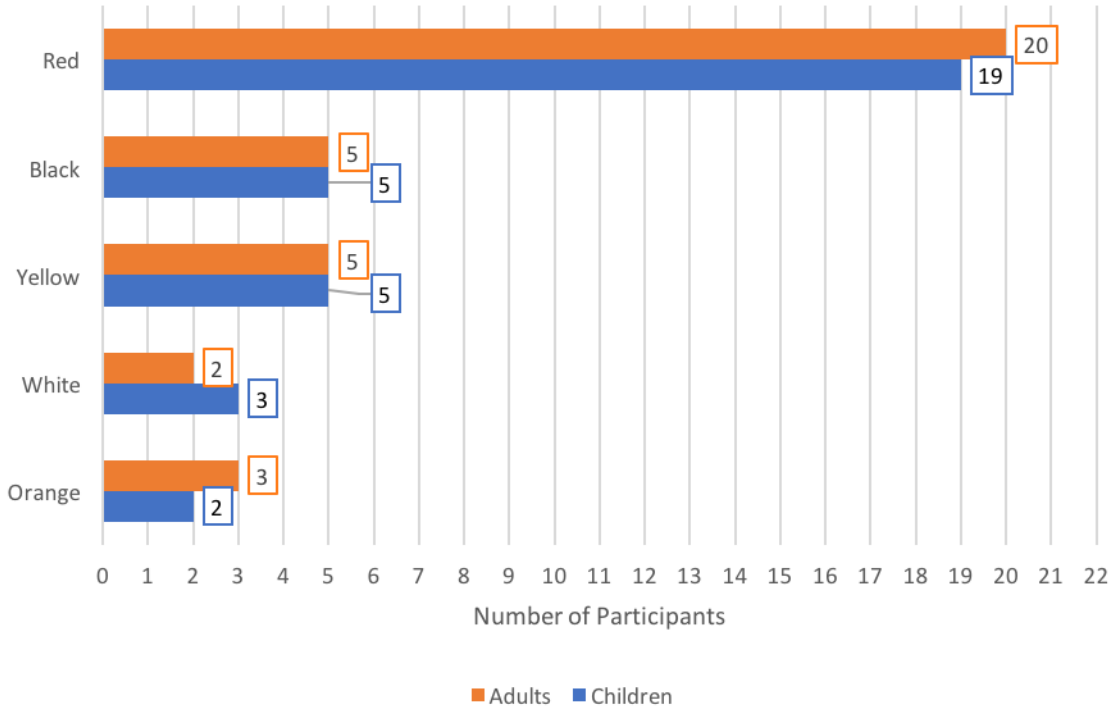


Figure 6.9: Comparison of children and adults' expectations for cybersecurity warning messages for colours.

like *visual cues that are bright, flashing, clear and noticeable*. Adults additionally suggested improved *risk communication*. Adults also expected to see warnings that appear *professional* and argued that this helps users to recognize that the warnings are legit and from a reputable source, similar to the findings from the literature on aesthetics and credibility [9, 49]. Two adults also wanted the warnings to *terminate the activity* that they recognize as dangerous without requiring any action from the users. This concept goes hand-in-hand with the idea of "human in the loop" and the importance of eliminating human-attributed security failures by automating components to perform security-critical functions when possible [13].

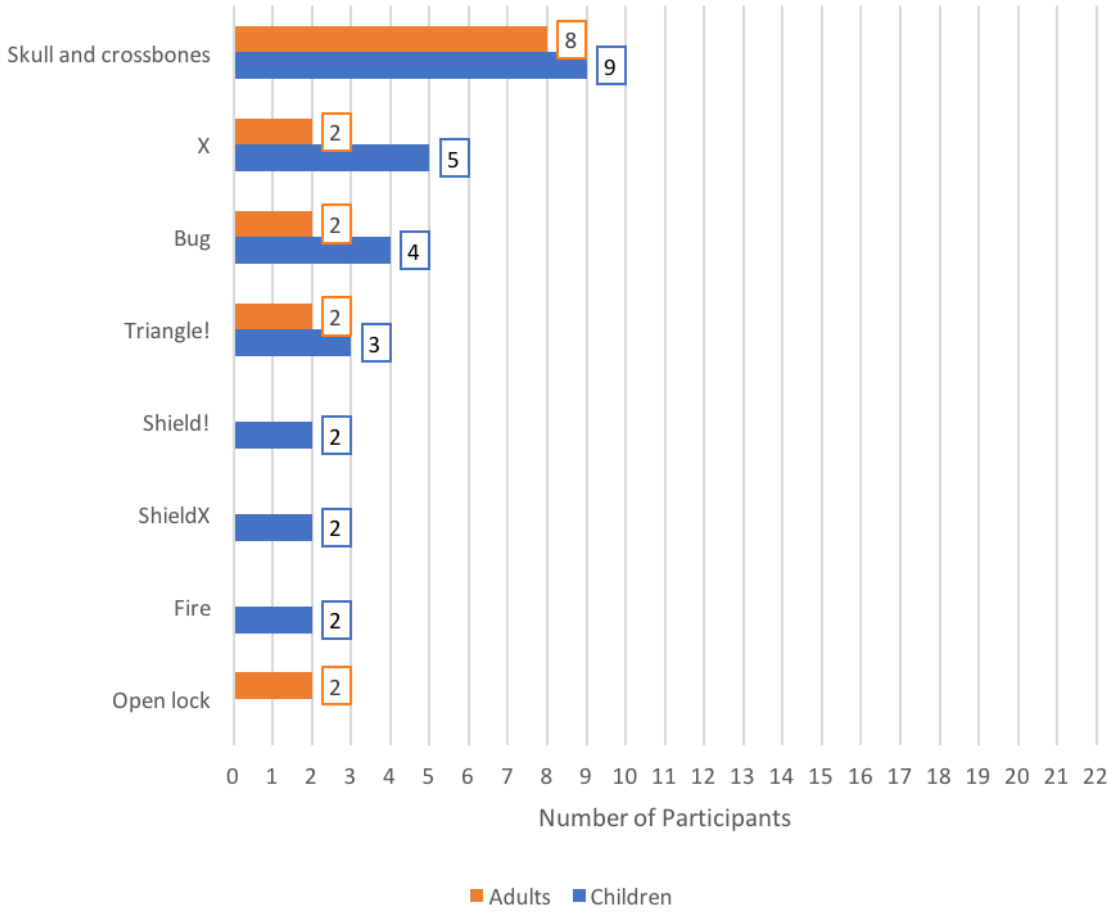


Figure 6.10: Comparison of children and adults' expectations for cybersecurity warning messages for symbols.

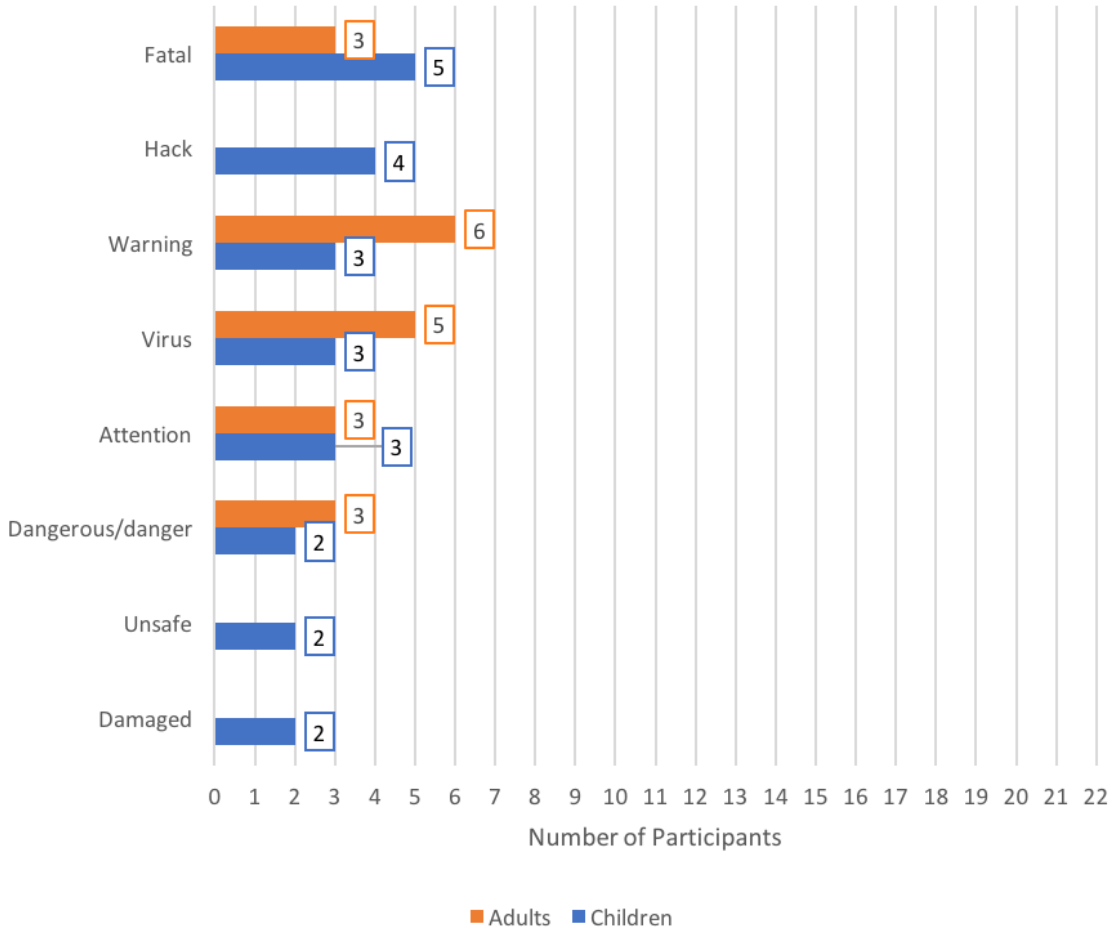


Figure 6.11: Comparison of children and adults' expectations for cybersecurity warning messages for words.

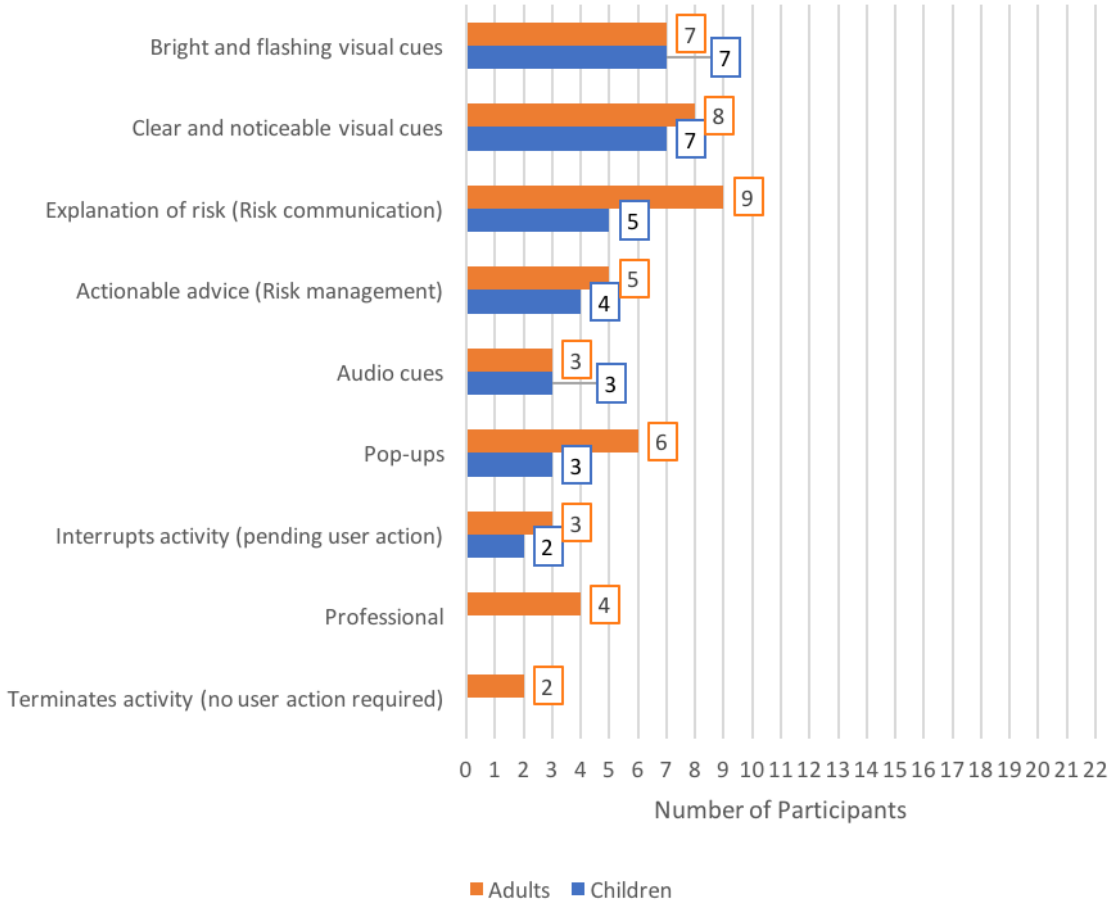


Figure 6.12: Comparison of children and adults' expectations for cybersecurity warning messages for other characteristics.

6.3 Secondary Findings

In our primary analysis, we set the threshold at n=2 for a theme to be recognized. Some of the single observations were nevertheless interesting, and may be useful to guide exploration in future studies. Due to the lack of literature comparing children and adults' perception of signal colours, symbols and words in the context of cybersecurity warnings, the followings observations will be discussed without the support of other research.

Children reported that they expected to see colours such as *navy*, *grey* and *blue*, and symbols like *angry face* and *sad face* on cybersecurity warnings to indicate something dangerous. Although children have many similar ideas with adults on which signal items imply danger, certain visual cues may communicate risk more effectively for children.

In their additional design suggestions for cybersecurity warnings, one adult participant proposed a *security threat scale*, an indicator that allows users to distinguish different threats and their severity of hazard:

> "I also prefer to have a little bit of guide, somewhere on top of it, like an indicator from green to very red. The colour of the pop-up depends on the danger, it might be different. I want to have an indicator to the top for colour and symbol, if it is this symbol how much it is dangerous. From green to red, a scale or guide to tell me how dangerous it is. The colour of the pop-up can be different depending on the danger. Skull and crossbones is most dangerous. Most safe can be happy face or thumbs up. It can start with word like 'unsafe' or 'fatal' and after that, tell me and give me some details of why I am not supposed to use this." **A10**

While useful, such a scale would be difficult to implement due to the high levels of uncertainty surrounding these risks. For example, if a risk is low probability and is shown as "green", would the few unlucky users who did succumb to the threat feel deceived?

Another adult participant proposed a *log or history of warnings* so that users can keep track of the warnings that they come across, and have access to the warning

when they exit out of it by mistake.

During the transcribing and coding process, we observed interesting secondary findings. Adults on average took longer to sort the cards, which could suggest a more complicated thought-process than children when it comes to determining the perceived severity of hazard for warning parameters. This may be due to adults having more complex existing mental models formed from learned conventions, past experiences and social norms. It is also possible that they were overthinking the activity. Adults were more hesitant and shy when they discussed the design parameters using contextual associations related to food and nature (e.g., *mint*, *olive*, *lime*, *orange*, etc.) for fear of seeming silly.

Adults' personal preferences and associations for colours were similar to that of children. Both groups mentioned their favourite colours and how that affected their perceptions when determining the severity of hazard of that particular colour. Some colours were regarded as "party colours" (e.g., pink, blue) and had positive connotations. These were likely to be considered safer than other colours.

Both groups found it difficult to assess single words without context. When sorting the words, participants talked about them in terms of full sentences. Some participants mentioned that they expected to see multiple signal words per warning. They wanted a clear explanation of how to proceed, what the problem is and precautionary measure that they could take. Some participants mentioned that words were not as effective in communicating risk on warnings because they are not universal. They believed that colours and symbols may be more appropriate for the general population. However, our findings suggest that this is not necessarily true. Some colours and symbols were interpreted differently depending on the individual's mental models, personal preferences, past experiences and cultural background, among other factors.

Chapter 7

Discussion and Conclusion

The goals of this thesis were to explore user perception of cybersecurity warnings and to provide design recommendations to effectively communicate risk to children. We revisit our main research question:

> "How do children and adults compare in their perceptions and understanding of signal colours, symbols, and words in the context of cybersecurity warning messages?"

To address this research question, we performed two user studies, one with children and another with adults, to examine how they perceive the severity of hazards associated with signal colours, symbols, and words in the context of cybersecurity warnings. We compared the studies and discovered similarities and differences between the two groups on their perceptions of, previous experiences with, and expectations for warning messages. The following sections highlight our contributions, recommendations and lessons learned. We conclude this thesis by discussing limitations of our studies and potential directions for future research.

7.1 Lessons Learned

We discuss the lessons we learned and insights gained from applying the human-in-the-loop (HITL) framework, following our research methodology, and conducting user studies with children and adults.

7.1.1 Applying Human-in-the-Loop

We found the *human-in-the-loop* (HITL) model [13] useful for framing the research question for our thesis. As Cranor [13] points out, when security-critical functions cannot be automated, we rely on humans to make judgments. In order to mitigate

human security failures, we need to build systems that are intuitive and effectively communicate risk. Through this framework, we were able to identify a research gap in the literature in the context of cybersecurity warnings. We identified a lack of empirical research providing design recommendations for cybersecurity warnings that effectively communicate risk to children. However, like previous studies on cyber warnings, we were able to address only some of the dimensions in the HITL framework [9] due to its broad scope. To improve warning design, we should also investigate the other steps of warning processing in future studies [9].

7.1.2 Research Methodology

Context

In our research, we gave participants a general security context where we asked them to imagine seeing a specific colour, symbol, or word on a cybersecurity warning message. Rather than providing our definition of cybersecurity warnings, we asked the participants to define them for us instead. We did so to discern how cybersecurity warnings were generally perceived by the users and if the users actually understood what the term meant. We also did not want to bias our participants' responses. Although the majority of participants primarily understood what warning messages were and gave appropriate definitions (e.g., warning dialogs, notices), they did not fully grasp what the warnings meant in the context of cybersecurity. They often interchangeably referred to security warnings and cyber warnings, and believed that cybersecurity warnings encompassed all digital warnings.

While some participants had no problem discussing design parameters in a general context, others needed to be reminded that these signal items were on a security warning. In our post-test interviews, we observed that both children and adults encountered *system status indicators* and *exception/error messages* that they interpreted as security warnings. While using a general context is helpful in avoiding researcher bias, it may also raise some misunderstanding and diverse interpretations from the participants. Future studies could benefit from giving participants specific security contexts to avoid this confusion. For example, investigating user perception when they receive cybersecurity warnings for expired SSL certificates or websites that

contain malware.

Card Sorting and Ranking Activities

Card sorting was a simple enough task for children aged 10 to 12 years old to successfully complete the activities. All participants were able to complete their study sessions. We asked the participants to first categorize the cards into three piles, and then to rank them within each category according to their perceived level of danger. By dividing the activities into two steps, we tried to avoid overloading participants.

We allowed participants to re-sort and re-categorize the cards throughout the sessions if they changed their minds. We only took photos of the final results of participants' card sorting. This helped the participants to systematically place the signal items in relation to one another. Some participants re-sorted the cards multiple times throughout the sessions. Adults on average took longer to sort the cards.

When participants thought two or more cards were equal in terms of their arousal strengths, we had to gently nudge them to choose and rank the signal items for our analysis. By using other methods that allow participants to allot defined values to the items, we may be able to avoid this situation, but may introduce other issues.

According to Hellier *et al.* [27], existing scales of arousal strength may be biased because they have not been validated across different methodologies. By using multiple techniques, researchers may alleviate the biases of a particular methodology. Likert-type rating, free modulus magnitude estimation and cross-modality matching [27] are a few other methodologies that may be used to scale the perceived arousal strengths [3, 26, 27, 64]. Hellier *et al.* [27] triangulated from three techniques, which provided both ratio and interval scaling data.

Aside from perceived level of hazard, Wogalter et al. [64] suggest other dimensions to evaluate warning effectiveness. Users' subjective measures on warnings such as perceived urgency or risk, likelihood of injury, likelihood of compliance, and importance can be taken on Likert-type scales. Participants can also rank warning effectiveness on the basis of dimensions that are self-selected [64]. We suggest that future studies use various techniques aside from categorizing and ranking activities. Mixed methods including both subjective and objective measures should be taken to evaluate warning

design. Along with the above mentioned subjective measures, researchers can collect data such as measurement of recall [64]. We suggest that with children, cross modality matching may be a good technique because participants need to simply draw a horizontal line to indicate the level of hazard implied by varying parameters.

Colour, Symbol and Word Selection

We investigated lists of 20 signal colours, 20 symbols, and 20 words. We included as many signal items as possible to provide an extensive comparison of perceived level of hazard.

As in common usage, some symbols such as circle, triangle and shield were presented in combination with ?, !, and X. Some participants had difficulty with these symbols that have an "icon within an icon". To categorize and rank, participants divided and dissociated the inner icons from the outer icons to explain their rationale.

On the cards for signal colours, we included the names of the colours below the coloured circles. By doing so, it was easier for analysis and for participants to name them. However, instead of referring to the colour itself, some participants associated the name of the colour. For example, participant **C18** mentioned that the colour lavender did not mean anything to him but the word lavender made him think of flowers. For future studies, we suggest putting the names of the colours on the back of the cards.

7.1.3 User Studies with Children and Adults

Children and adults are fundamentally different in their psychology, perception and mental models [66, 67]. Our results indicate that generally, both groups had similar responses. They had similar ideas on which signal colours, symbols, and words indicated most danger and safety. Some differences observed pertained to personal preferences for colours (e.g., adults preferred *black* more than children), attitudes towards signal items (e.g., children generally discussed *police officer or security guard* in a more positive light than adults), and the simplicity in the rationale of the card placements (e.g., a few children gave one-word or one-sentence responses using associations they made without providing further explanation even when probed).

7.2 Recommendations

Our research provides preliminary data on children's perception of signal colours symbols, and words in the context of cybersecurity warnings. Based on our findings from the user studies and reflecting on them in light of the literature, the following design suggestions have been developed.

7.2.1 Simple and Basic Design Parameters

Simple and basic signal colours, symbols, and word are recommended to effectively communicate risk to users in the context of cybersecurity warnings. We recommend designers to use signal items that are ranked higher (most dangerous) and ranked lower (safest) on the ordinal scales, and top 3 expected signal colours, symbols and words on warnings because they have lower likelihood of being misinterpreted by users. Others may be easily misinterpreted due to individual differences.

To design warnings indicating danger for children, we recommend signal colours such as *red*, *black*, *maroon* and *yellow*, signal symbols such as *skull and crossbones*, *bug* and *X*, and signal words such as *fatal*, *hack*, *virus* and *warning*.

To convey safety, signal colours such as *green*, *cyan*, and *lime*, signal symbols such as *happy face* and *police officer/security guard*, and signal words such as *protect*, *security* and *online* are recommended.

We also suggest designers to stay away from symbols that can cause confusion and misinterpretation such as the lock symbol. Unlike the *happy face* and *sad face*, our results show that the binary relationship of *open lock* and *closed lock* was easily misinterpreted. Both children and adults had mixed notions on how dangerous or safe these symbols were.

Many cybersecurity warning messages contain technical terms and computer jargon that are difficult for users to understand [9]. Some participants mentioned the importance of keeping the words simple and easy because the general population do not understand technical terms and computer jargon such as error codes. This idea particularly applies to children, who may have less advanced vocabulary.

Peters [49] suggests strategies for simplifying visuals such as using symbols, removing extra detail, clearing the background, and making text legible, concise and

consistent.

7.2.2 Warning Design Guidelines for Children

We adapted the aforementioned set of warning design guidelines by Bauer *et al.* [5] (Section 2.3.3) using insights from our studies and existing literature, and recommendations from other guidelines for children [43].

We suggest the following set of guidelines, with our additions and modifications in ***bold***:

1. *Describe the risk comprehensively*: The risk should be clearly identified and explained. ***Warning messages should make it clear who is doing what to whom, explain the consequences of noncompliance, and provide instructions on how to comply so that children could easily understand them.***

2. *Be concise and accurate*: The warning messages should be simple, to the point, give correct information and minimize technical terms and computer jargon. ***They should provide informative headings, include short paragraphs, use simple sentences, and avoid confusing language such as double negatives so that children could easily read them.***

3. *Offer meaningful options*: Warning dialogs should provide users with sufficient information so that they can decide between two or more meaningful options. The default option should always be the safer choice and corresponds to the question asked or information given. ***When the situation is too risky, children should be provided with actionable advice such as encouraging them to report the warnings to their parents or responsible adults.***

4. *Present relevant contextual information*: Warnings should present contextual information such as the consequences of noncompliance, so that users can make informed decision. ***If applicable, the security-critical functions should***

be automated to remove the onus from the children, such as running an antivirus program first and terminating activity without requiring user action.

5. *Present relevant auditing information*: The user's device should maintain access logs and the warning should show whether the website or the application has been previously accessed. ***When children exit out of the warnings by mistake, they should be able to go back and access the warnings to read the information that they missed or to show them to their parents or adults.***

6. *Follow a consistent layout*: Warnings should follow a common suggested layout based on the Human Interface Guidelines (HIG) [29, 50, 61]. These elements include a single icon, primary text, secondary text, a question, a set of primary options, and a set of secondary options. ***Information should be arranged in a logical order and the main idea of the sentence should be placed at the beginning so that they can be recognized easily by children.***

7. ***Provide other visual and audio cues: To increase salience, warnings that indicate immediate danger should have clear, noticeable, bright and flashing visual cues, and audio cues if necessary.***

8. ***Use, but do not overuse, emphasis techniques: When used appropriately, emphasis techniques such as colour, indentation, size, shape and boldface can enhance comprehension. Related information should be grouped together and redundancies should be eliminated using signal colours, symbols, and words that effectively communicate appropriate risk to children.***

9. ***Use simple design parameters: Use simple and basic signal colours, symbols and words that appropriately communicate the level of hazard for children. Avoid signal items that can be misinterpreted.***

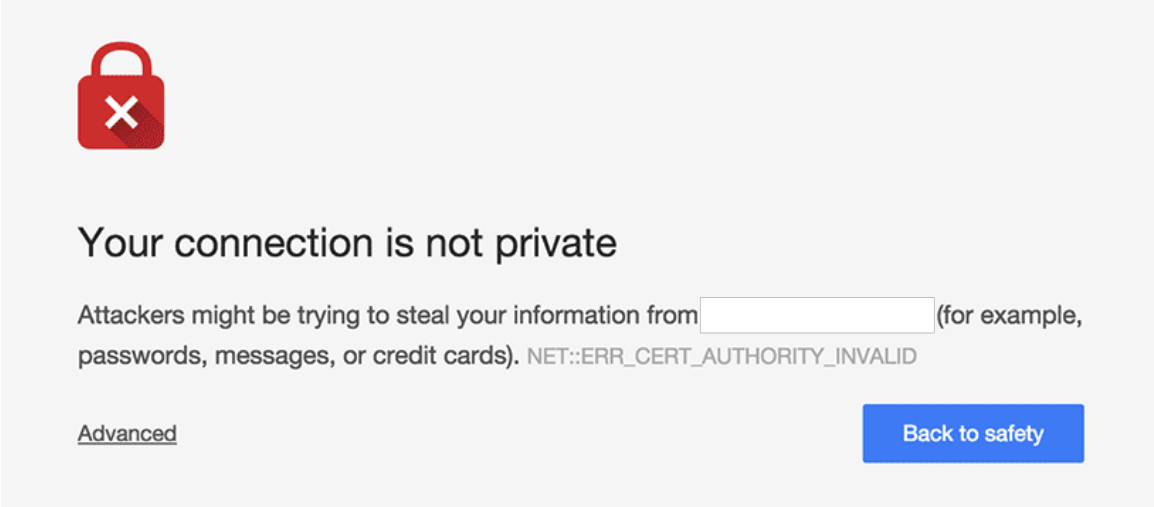


Figure 7.1: An example of SSL certificate for Google Chrome.

7.2.3 Application to Real Warnings

We provide an example of how these recommendations for children may apply to real warnings. Consider the SSL certificate for Google Chrome in Figure 7.1.

The colour *red* is used to signal danger in the warning, which aligns with our suggestion for children. However, while the symbol X conveys danger and may effectively communicate risk to children, our findings show that the *closed lock* symbol may cause confusion and misinterpretation. It may be more effective to simply use the X symbol only, or in combination with a signal word such as *warning*.

The language used on this Google Chrome SSL certificate may be appropriate for children 10 to 12 years old because it does not contain overly technical terms and computer jargon, with the exception of the error codes. The language may be difficult to understand depending on children's reading comprehension level, which needs to be considered for future studies. We believe that the warning may be more effective without the error codes. If the parents or responsible adult want more information on the warning, the error codes may be moved under the "advanced" option. We suggest that the error code be replaced by an encouragement for children to show this warning to their parents or responsible adults.

7.3 Limitations

We traded ecological validity for a more controlled lab setting that enabled us to test a large number of items. However, this meant sacrificing some context. Participants may respond differently when faced with these signal items as part of an actual cybersecurity warning and in response to some event on their device. Our results can be used to inform follow-up studies by providing a subset of signal items that are most likely effective.

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.

In our user studies, we did not ask participants to quantify the arousal strengths, so we do not know the exact differences between the values of items. Instead, we can say that we have produced ordinal scales or ranked lists of signal colours, symbols and words in the order of *rank 1 = most safe* to *rank 20 = most dangerous*. The differences between items are not really known. Since this was a first attempt at scaling the level of hazard for signal colours, symbols and words, future studies could test replicability and generalizability of these scales and to establish more robust scales.

In the three categories for the card sorting activity, we had a middle sign that said "neither safe nor dangerous". When we ran our sessions, we verbally clarified that the signal items placed in this category are "both" or "neither safe nor dangerous". For future studies, we should correct the sign to avoid confusion.

In this thesis, we focused on two user groups, children aged 10 to 12 years old 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 various signal colours, symbols, and words. Future studies may benefit from considering participants from varying demographics such as age, gender, and cultural and economical background.

7.4 Future Work

The findings from our thesis opens new avenues for future exploration into user perception of cybersecurity warning design parameters.

Other research on warnings and images [47] found that users were much more likely be pay attention to messages with symbols than those relying solely on text-only messages. On the other hand, the combinations of colours with signal words suggested by warning standards were not well supported by the findings by Griffith and Leonard [25, 36], none looked at children's understanding. Future studies may benefit from exploring combinations of signal colours, symbols, and words on children's risk perception.

In this research, we focused on warning design features that are visual. Some of our participants suggested adding audio cues for more effective risk communication. Auditory warnings may be useful when we need to call for attention, the visual environment is cluttered, and the message is simple [64]. Future studies may benefit from exploring non-visual features such as auditory cues on security warnings for more salience.

As proposed by participant **A10**, a security threat scale may be useful for users to distinguish between safe and dangerous warnings, and warnings with varying severity of hazard. The safe and dangerous warnings can be differentiated by different colours such as *green* for *safe* and *red* for *dangerous*, while the *varying severity of hazard* can be communicated through visual hierarchy using *variations in tone* of colours. As suggested by Peters [49], the greater the saturation in tone, the greater the severity. As mentioned in the previous chapter, there is a high degree of uncertainty surrounding risks. This may be further explored to test the plausibility and usefulness of such scales.

7.5 Contributions

We aimed to partially address the gap in the literature on children and cybersecurity warnings. In this thesis, we investigated a number of questions about user perception and warning design parameters. To re-iterate, we make the following contributions:

1. Through our card sorting and ranking activities, we provided ordinal scales and preliminary data on relationships between user's perceived level of hazard and warning design parameters using a comprehensive list of 20 signal colours, 20 symbols, and 20 words. Once these findings are further explored and replicated through future studies using various research methodologies, these scales may be used by cybersecurity practitioners to achieve hazard matching.

2. We investigated adults' perceptions as a baseline for comparison because current cybersecurity warnings are typically designed for adult users. From our two user studies with 22 child participants and 22 adult participants, we identified how children and adults compare in their perceptions of, previous experiences with, and expectations for cybersecurity warning design parameters.

3. We identified some concepts and associations that shaped children and adults' risk perceptions, and helped them to determine what is dangerous or safe when it comes to signal colours, symbols, and words.

4. We adapted the warning design guidelines by Bauer *et al.* [5] to provide recommendations to consider when developing cybersecurity warning messages for children. These may be used by cybersecurity designers and developers to inform the design of warnings or to evaluate those that are currently implemented.

7.6 Conclusion

Although much research has been conducted on warning messages with adults, their responses may not accurately reflect the needs of children. We wanted to address this research gap and work towards cybersecurity warning messages that effectively communicate risk to children. We conducted two user studies and uncovered similarities and differences between children and adults' perception of signal colours, symbols, and words. Our results, combined with the evidence from the literature, suggest that users' perceived level of hazard may be highly dependent on personal preferences and past experience with the design parameters. However, we found high agreement on certain signal items at the extreme ends of the scale, suggesting a subset of signal items that are unambiguous for both children and adults.

Bibliography

[1] Devdatta Akhawe and Adrienne P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., 2013. USENIX.

[2] Hazim Almuhimedi, Adrienne P. Felt, Robert W. Reeder, and Sunny Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 113–128, Menlo Park, CA, 2014. USENIX Association.

[3] T. S. Amer and JoMae B. Maris. Signal words and signal icons in application control and information technology exception messageshazard matching and habituation effects. *Journal of Information Systems*, 21(2):1–25, 2007.

[4] Bonnie B. Anderson, C. Brock Kirwan, Jeffrey L. Jenkins, David Eargle, Seth Howard, and Anthony Vance. 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, pages 2883–2892, New York, NY, USA, 2015. ACM.

[5] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. Warning design guidelines. Technical Report CMU-CyLab-13-002, CyLab, Carnegie Mellon University, February 2013.

[6] C. J. Boyatzis and Ramani Varghese. Children's emotional associations with colors. *The Journal of genetic psychology*, 155 1:77–85, 1994.

[7] Curt C. Braun, Paul B. Mine, and N. Clayton Silver. The influence of color on warning label perceptions. *International Journal of Industrial Ergonomics*, 15(3):179 – 187, 1995.

[8] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Harder to ignore? revisiting pop-up fatigue and approaches to prevent it. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 105–111, Menlo Park, CA, 2014. USENIX Association.

[9] Cristian Bravo-Lillo, Lorrie F. Cranor, Julie S. Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[10] Cristian Bravo-Lillo, Lorrie F. Cranor, Julie S. Downs, Saranga Komanduri, and Manya Sleeper. Improving computer security dialogs. In *Proceedings of the 13th*

IFIP TC 13 International Conference on Human-computer Interaction - Volume Part IV, INTERACT'11, pages 18–35, Berlin, Heidelberg, 2011. Springer-Verlag.

[11] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie F. Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 6:1–6:12, New York, NY, USA, 2013. ACM.

[12] L. J. Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3):37–46, 2009.

[13] Lorrie F. Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, pages 1:1–1:15, Berkeley, CA, USA, 2008. USENIX Association.

[14] Julia Davidson and Elena Martellozzo. Exploring young people's use of social networking sites and digital media in the internet safety context: A comparison of the uk and bahrain. *Information, Communication & Society*, 16:1–21, 01 2012.

[15] Satu Elo and Helvi Kyngs. The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1):107–115, 2008.

[16] Michael Fagan, Mohammad M.H. Khan, and Nhan Nguyen. 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):36, Dec 2015.

[17] Adrienne P. Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving ssl warnings: Comprehension and adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2893–2902, New York, NY, USA, 2015. ACM.

[18] Adrienne P. Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa E. Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, Denver, CO, 2016. USENIX Association.

[19] Georgios D. Floros, Konstantinos E. Siomos, Virginia Fisoun, Evaggelia Dafouli, and Dimitrios Geroukalis. Adolescent online cyberbullying in greece: The impact of parental online security practices, bonding, and online impulsiveness. *Journal of School Health*, 83(6):445–453, 2013.

[20] Canadian Centre for Occupational Health and Safety. Whmis 2015 – labels. https://www.ccohs.ca/oshanswers/chemicals/whmis_ghs/labels.html, 2015.

[21] Canadian Centre for Occupational Health and Safety. Whmis 2015 fact sheets. https://www.ccohs.ca/products/publications/whmis_ghs/, 09 2016.

[22] Jana Fruth, Ronny Merkel, and Jana Dittmann. *Security Warnings for Children's Smart Phones: A First Design Approach*, pages 241–243. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[23] Andrew J.B. Fugard and Henry W.W. Potts. Supporting thinking on sample sizes for thematic analyses: a quantitative tool. *International Journal of Social Research Methodology*, 18(6):669–684, 2015.

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

[25] L.J. Griffith and S. David Leonard. Association of colors with warning signal words. *International Journal of Industrial Ergonomics*, 20(4):317–325, 1997.

[26] Elizabeth Hellier, Kirsteen Aldrich, Daniel B. Wright, Denny Daunt, and Judy Edworthy. A multi dimensional analysis of warning signal words. *Journal of Risk Research*, 10(3):323–338, 2007.

[27] Elizabeth Hellier, Daniel B. Wright, Judy Edworthy, and Stephen Newstead. On the stability of the arousal strength of warning signal words. *Applied Cognitive Psychology*, 14(6):577–592, 2000.

[28] Linda Holtzschue. *Understanding color: an introduction for designers*. Wiley, 5 edition, 2017.

[29] Apple Inc. Apple human interface guidelines. https://developer.apple.com/design/human-interface-guidelines/macos/overview/themes, 2018.

[30] QSR International. What is nvivo? https://www.qsrinternational.com/nvivo/what-is-nvivo, 2018.

[31] Yousra Javed and Mohamed Shehab. Look before you authorize: Using eye-tracking to enforce user attention towards application permissions. *Proceedings on Privacy Enhancing Technologies*, (2):23–37, 04 2017.

[32] Michael Kalsher and K. Williams. Behavioral compliance: Theory, methodology, and result. *Handbook of Warnings*, pages 313–331, Lawrence Erlbaum Associates, 2006.

[33] Naz Kaya and Helen H. Epps. Color-emotion associations: Past experience and personal preference. *AIC 2004 Color and Paints, Interim Meeting of the International Color Association, Proceedings*, 5, 01 2004.

[34] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology (second edition)*. Sage Publications, 2004.

[35] Kaspersky Lab. Kaspersky security bulletin: Overall statistics for 2017. Technical report, Kaspersky Lab, December 2017.

[36] S. David Leonard. Does color of warnings affect risk perception? *International Journal of Industrial Ergonomics*, 23:499–504, 03 1999.

[37] Qingguo Ma, Xiaoxu Bai, Guanxiong Pei, and Zhijiang Xu. The hazard perception for the surrounding shape of warning signs: Evidence from an event-related potentials study. *Frontiers in Neuroscience*, 12:824, 2018.

[38] Greg Masters. Crying wolf: Combatting cybersecurity alert fatigue. `https://www.scmagazine.com/home/security-news/in-depth/crying-wolf-combatting-cybersecurity-alert-fatigue/`, 6 2017.

[39] Common Sense Media. The common sense census: Media used by kids age zero to eight, 2017. `https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf`, 2017.

[40] MediaSmarts. Internet safety tips by age: 11-13. `http://mediasmarts.ca/tipsheet/internet-safety-tips-age-11-13`, 2014.

[41] MediaSmarts. Internet safety tips by age: 8-10. `http://mediasmarts.ca/tipsheet/internet-safety-tips-age-8-10`, 2014.

[42] Wiebke Menzel, Sven Tuchscheerer, Jana Fruth, Christian Kraetzer, and Jana Dittmann. 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, 2012.

[43] Anca Micheti, Jacquelyn Burkell, and Valerie Steeves. Fixing broken doors: Strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology & Society*, 30(2):130–143, 2010.

[44] Granger M. Morgan, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman. *Risk Communication: A Mental Models Approach*. Cambridge University Press, 2001.

[45] Ajaya Neupane, Nitesh Saxena, Keya Kuruvilla, Michael Georgescu, and Rajesh K. Kana. Neural signatures of user-centered security: An fmri study of phishing, and malware warnings. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*, 2014.

[46] Ministry of Transportation. 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.

[47] Michelle O'Hegarty, Linda L. Pederson, David E. Nelson, Paul Mowery, Julia M. Gable, and Pascale Wortley. Reactions of young adult smokers to warning labels on cigarette packages. *American Journal of Preventive Medicine*, 30(6):467 – 473, 2006.

[48] Shirley M. Otsubo. A behavioral study of warning labels for consumer products: Perceived danger and use of pictographs. *Proceedings of the Human Factors Society Annual Meeting*, 32(9):536–540, 1988.

[49] Dorian Peters. *Interface Design for Learning: Design Strategies for Learning Experiences*. New Riders, 2014.

[50] The GNOME Project. Gnome human interface guidelines. `http://library.gnome.org/devel/hig-book/stable/index.html.en`, 2014.

[51] Niels Provos. Safe browsing – protecting web users for 5 years and counting. `https://security.googleblog.com/2012/06/safe-browsing-protecting-web-users-for.html`, 6 2012.

[52] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le C. Wang, and Konstantin Beznosov. A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 1:1–1:20, New York, NY, USA, 2011. ACM.

[53] Mario Silic, Dianne Cyr, Andrea Back, and Adrian Holzer. Effects of color appeal, perceived risk and culture on user's decision in presence of warning banner message. In *HICSS*, 2017.

[54] Valerie Steeves. Young canadians in a wired world, phase iii: Life online. `http://mediasmarts.ca/ycww/life-online`, 2014.

[55] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie F. Cranor. Crying wolf: An empirical study of ssl warning effectiveness. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, pages 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[56] Shauna Tominey and Megan Mcclelland. Red light, purple light: Findings from a randomized trial using circle time games to improve behavioral self-regulation in preschool. *Early Education and Development*, 22:489–519, 05 2011.

[57] Lisa Vaas. Google redesigns security warnings after 70% of chrome users ignore them. `https://nakedsecurity.sophos.com/2015/02/03/google-redesigns-security-warnings-after-70-of-chrome-users-ignore-them/`, 2 2015.

[58] Anthony Vance, Brock Kirwan, Daniel Bjornn, Jeffrey Jenkins, and Bonnie B. Anderson. What do we really know about how habituation to warnings occurs over time?: A longitudinal fmri study of habituation and polymorphic warnings. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 2215–2227, New York, NY, USA, 2017. ACM.

[59] Johannes Wheeldon and Jacqueline Faubert. Framing experience: Concept maps, mind maps, and data collection in qualitative research. *International Journal of Qualitative Methods*, 8(3):68–83, 2009.

[60] Alma Whitten and J.D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, Berkeley, CA, USA, 1999. USENIX Association.

[61] Microsoft Windows. Windows design guidelines. `https://docs.microsoft.com/en-us/windows/desktop/uxguide/guidelines`, 2018.

[62] Michael S. Wogalter. Communication-human information processing model. *Handbook of Warnings*, pages 51–61, Lawrence Erlbaum Associates, 2006.

[63] Michael S. Wogalter. Proposes and scope of warnings. *Handbook of Warnings*, pages 3–9, Lawrence Erlbaum Associates, 2006.

[64] Michael S. Wogalter, Vincent C. Conzola, and Tonya L. Smith-Jackson. Research-based guidelines for warning design and evaluation. *Applied Ergonomics*, 33:219–230, 2002.

[65] Yan Zhang and Barbara M. Wildemuth. Qualitative analysis of content. *Applications of Social Research Methods to Questions in Information and Library Science*, 01 2009.

[66] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction, Elsevier*, 2017. Articles.

[67] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*, IDC '16, pages 388–399, New York, NY, USA, 2016. ACM.

Appendix A

Definitions

- **Active communications**: interrupt users' activity so that they pay attention [13].
- **Arousal strength**: the severity/level of hazard communicated by the warning or design parameters [3].
- **Attention maintenance**: users maintaining their attention to the communication long enough to process it [13].
- **Attention switch**: users taking notice of the communication [13].
- **Clickthrough rate**: the proportion of users who clicked through a warning type by ignoring or making an informed decision to proceed [1].
- **Communication delivery**: the first step in information processing that includes attention switch and attention maintenance [13].
- **Cyber warnings**: synonymous with digital warnings.
- **Cybersecurity warnings**: digital warnings pertaining to security.
- **Design parameter**: individual design components including signal colours, words and symbols, terminology as first used by Amer and Maris [3] (also known as design elements).
- **Hazard matching**: successfully mapped risk to warnings, where the severity of the hazard that is implied by the warning message should match the level of hazard perceived by the user [3, 27].

- **Human-receiver**: the human who receives the security communication and whose actions affect system security [13] (also known as the user or the human-in-the-loop).

- **Notices**: provide users information and characteristics of entity or object (e.g., privacy polices, SSL certs) [13].

- **Passive communications**: provide information to users without actively trying to get their attention [13].

- **Security metaphor**: an association that is used to explain a particular element of a system based on an expert understanding, referred to as "mental models" by Camp [12].

- **Severity of hazard**: synonymous with level of hazard.

- **Signal colours/words/symbols**: design parameters that signal potential hazards to users encountering potentially harmful situations [3].

- **Signal item**: any singular signal colour, word or symbol.

- **Status indicators**: inform users about system status or the risk condition (e.g., taskbar and menu bar indicators about bluetooth, virus software up-to-date, file permissions [13].

- **Theory of warning fatigue**: when users become desensitized to the stimulus as they continue to receive more and more warnings [1, 38].

- **Warning dialogs**: alert users to take immediate action to avoid a threat (e.g., anti-phishing, expired SSL certs) [13].

- **Warning effectiveness**: how effectively the warning communicates risk [1].

Appendix B

Complete List of Cards

B.1 List of Cards

Table B.1 summarizes the complete list of 60 cards used during card sorting and ranking activities.

Card	Words	Colours	Symbols
01	Alert	Red	Open lock
02	Attention	Pink	Closed lock
03	Blocked	Orange	Happy face
04	Careful	Yellow	Sad face
05	Damage	Green	Angry face
06	Don't	Blue	Bug
07	Error	Black	Key
08	Fatal	Grey	Security guard or Police officer
09	Hack	White	Fire
10	Important	Maroon	Skull and crossbones
11	Message	Brown	Stop hand
12	Notice	Coral	Shield with !
13	Online	Olive	Shield with ?
14	Protect	Lime	Shield with X
15	Security	Mint	Triangle with !
16	Suspicious	Cyan	Triangle with ?
17	Unsafe	Navy	Triangle with X
18	Urgent	Purple	Circle with !
19	Virus	Lavender	Circle with ?
20	Warning	Magenta	Circle with X

Table B.1: List of cards.

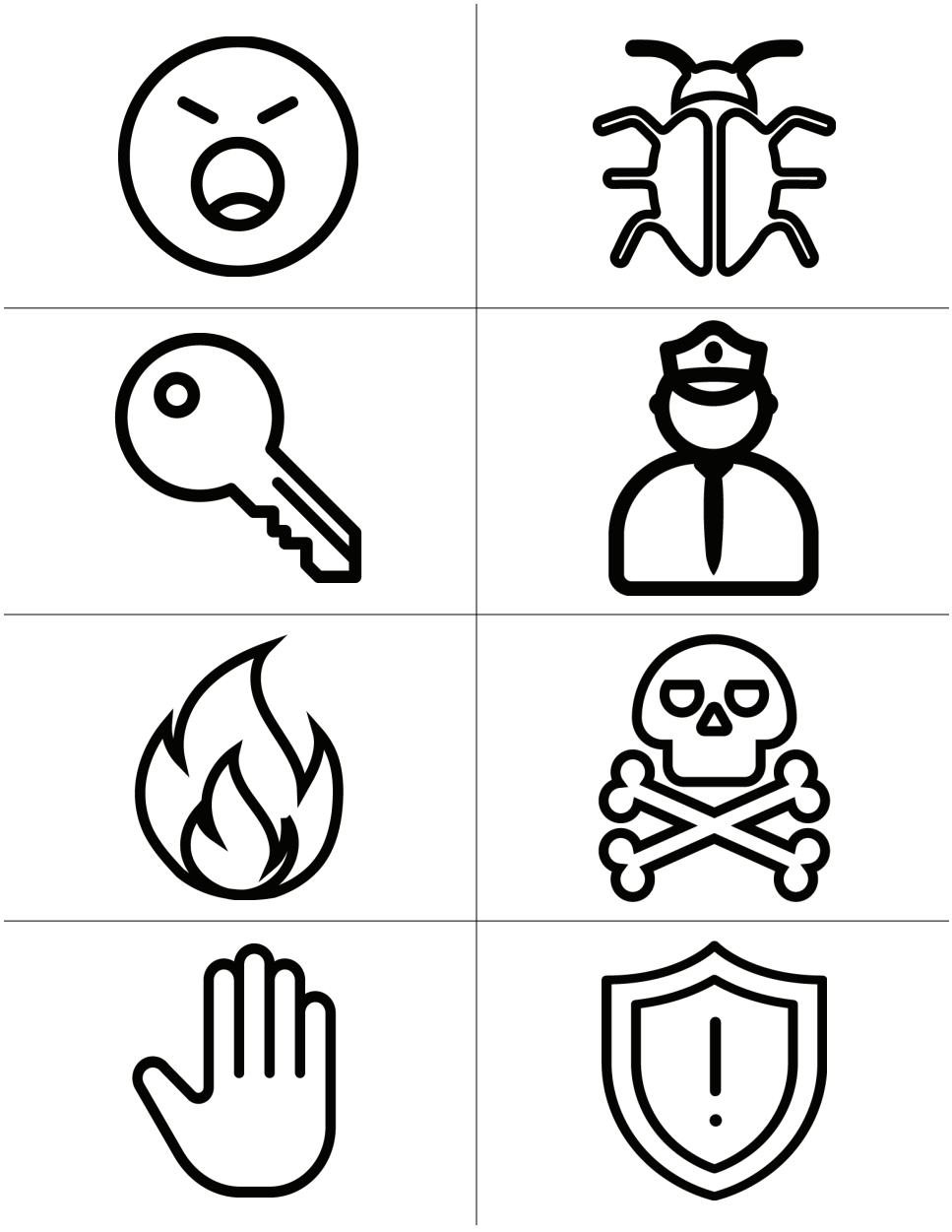
B.2 Cards Template

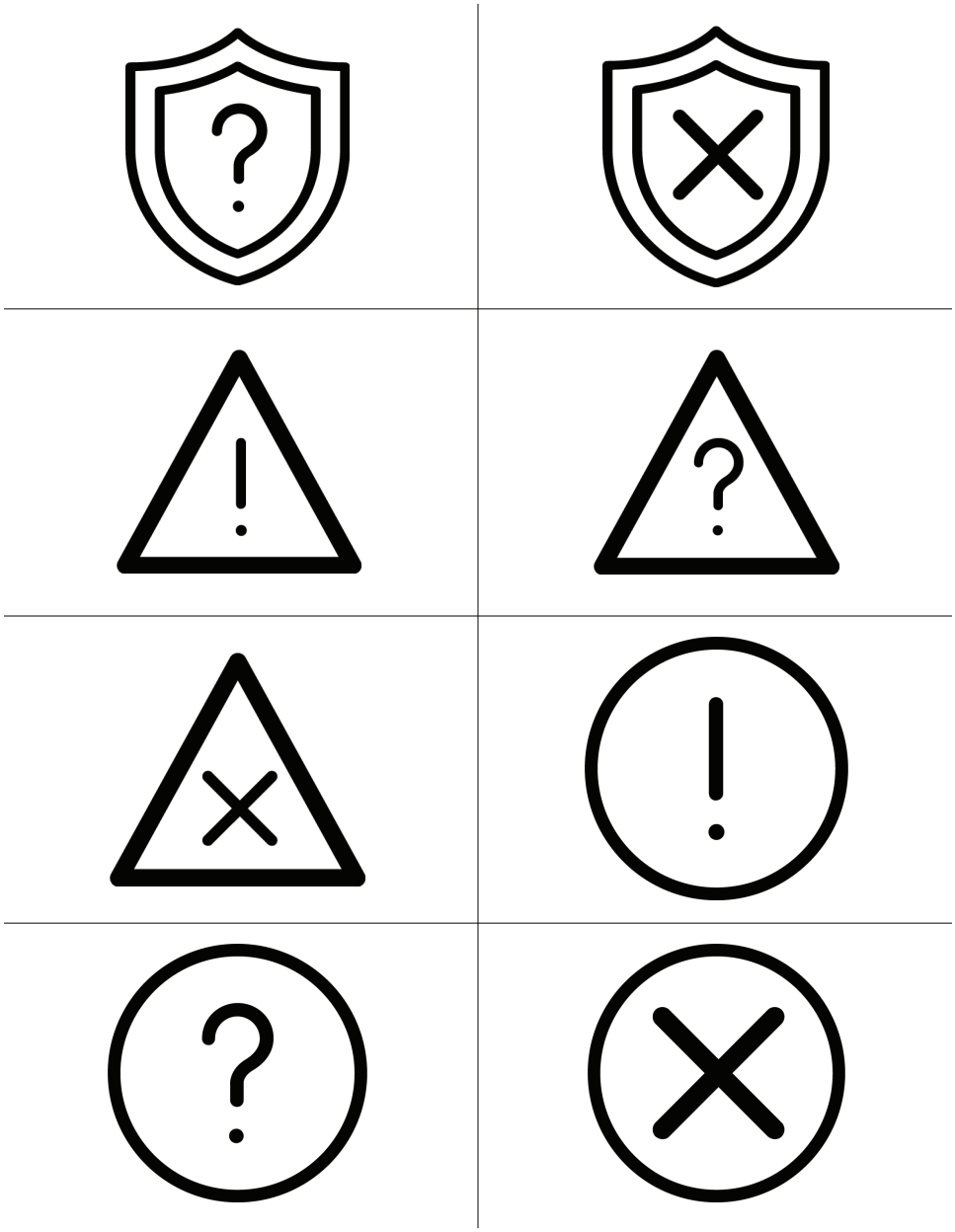
The figure below is the template of the cards used during card sorting and ranking activities.

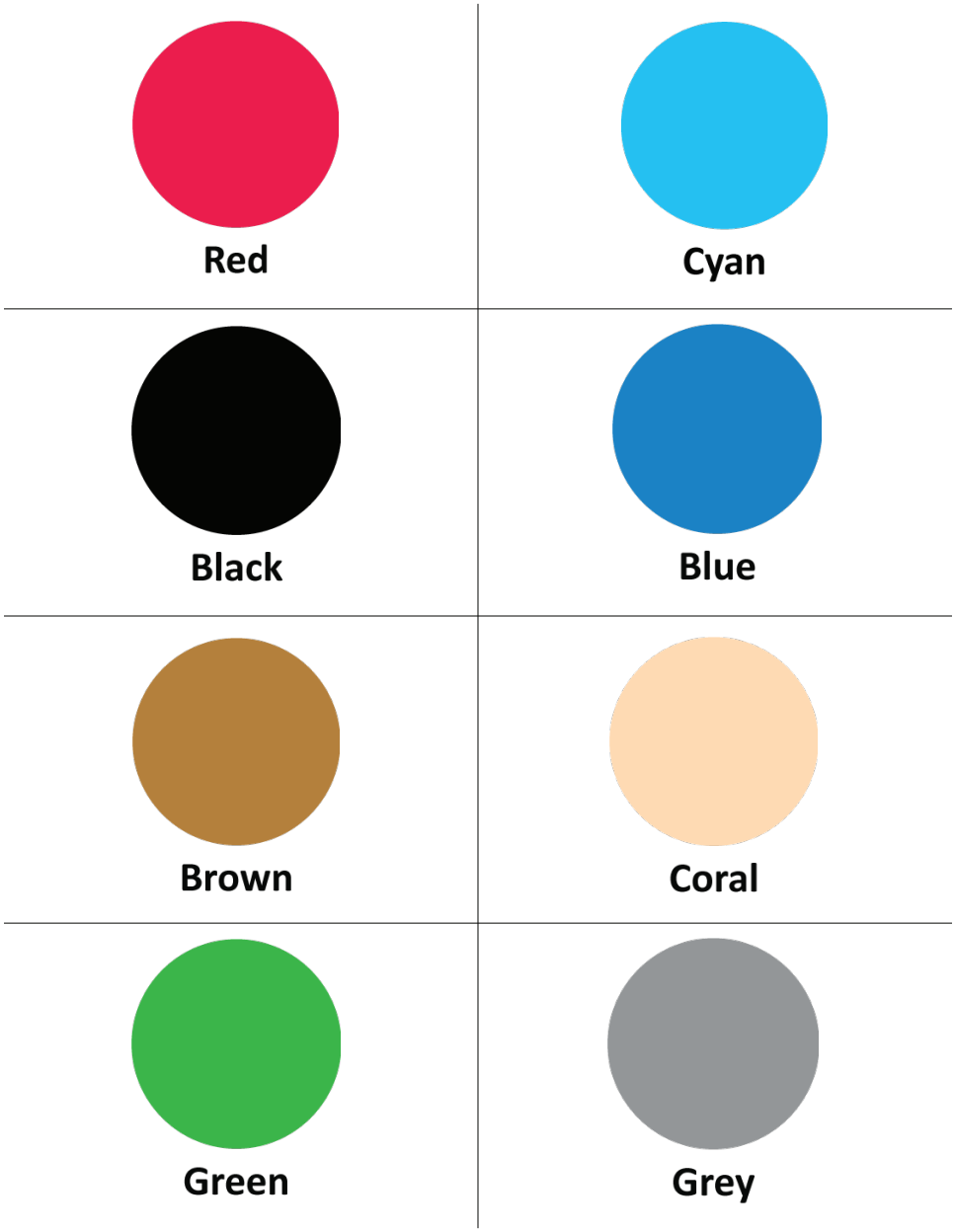
Alert	Attention
Blocked	Careful
Damage	Don’t
Error	Fatal

Hack	Important
Message	Notice
Security	Suspicious
Online	Protect

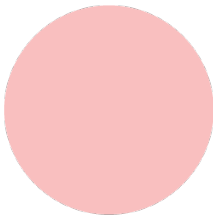
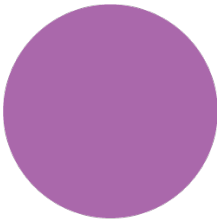
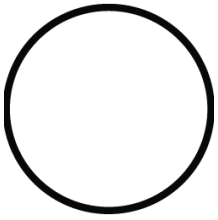
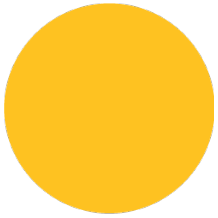
Unsafe	Urgent
Virus	Warning
	
	






Red
Cyan
Black
Blue
Brown
Coral
Green
Grey


Lavender
Lime
Magenta
Maroon
Mint
Navy
Olive
Orange

 Pink	 Purple
 White	 Yellow

Appendix C

Recruitment Materials

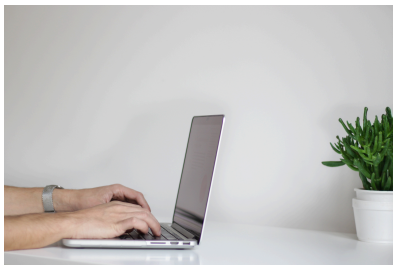
Carleton UNIVERSITY
Canada's Capital University

Recruitment Poster: Sample

Looking for children volunteers:

Exploring characteristics of cybersecurity warning messages

We are looking for volunteers for a research study that explores different characteristics of cybersecurity warning messages to understand how children interpret them.



Children participants will complete sorting activities and answer some questions. The study will take approximately 1 hour.

Eligibility: Children aged 10-12 years old comfortable speaking and reading in English.

Compensation: $20 cash.

If you are interested in participating, please email Rebecca at:
rebecca.jeong@carleton.ca

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

ybersecurity Warning Messages *ebecca.jeong@carleton.ca*

Carleton UNIVERSITY
Canada's Capital University

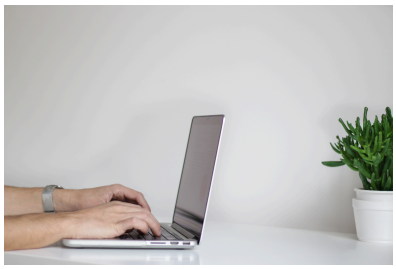
Adult Recruitment Poster: Sample

Looking for volunteers:

Exploring characteristics of cybersecurity warning messages

We are looking for volunteers for a research study that explores different characteristics of cybersecurity warning messages to understand how we interpret them.

Participants will complete sorting activities and answer some questions. The study will take approximately 1 hour.



Eligibility: Adults over 18 years old comfortable speaking and reading in English.

Compensation: $20 cash.

If you are interested in participating, please email Rebecca at:
rebecca.jeong@carleton.ca

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

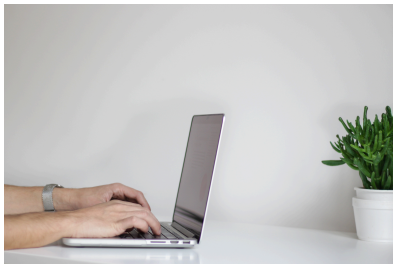
ybersecurity Warning Messages *ebecca.jeong@carleton.ca*

Carleton UNIVERSITY
Canada's Capital University

Social Media Recruitment: Sample

Looking for children volunteers:

Exploring characteristics of cybersecurity warning messages



I am a Masters student at Carleton University, working under the supervision of Dr. Sonia Chiasson.

We are looking for volunteers for a research study. Each participant will be rewarded for their time with $20 cash.

This study will explore different characteristics of cybersecurity warning messages to understand how children interpret them.

As a participant in this study, your child will complete sorting activities and answer some questions. The study will take approximately 1 hour.

We are looking for children between the ages of **10 to 12 years old**, comfortable speaking and reading in English.

If you are interested in participating, please e-mail Rebecca at:
rebecca.jeong@carleton.ca

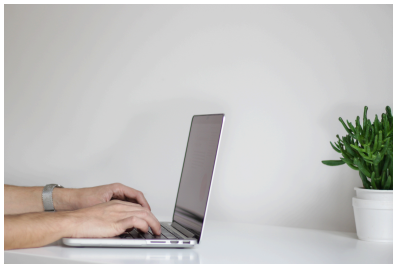
This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

Carleton UNIVERSITY
Canada's Capital University

Adult Social Media Recruitment: Sample

Looking for volunteers:

Exploring characteristics of cybersecurity warning messages



I am a Masters student at Carleton University, working under the supervision of Dr. Sonia Chiasson.

We are looking for volunteers for a research study. Each participant will be rewarded for their time with $20 cash.

This study will explore different characteristics of cybersecurity warning messages to understand how we interpret them.

As a participant in this study, you will complete sorting activities and answer some questions. The study will take approximately 1 hour.

We are looking for adult volunteers over **18 years old**, comfortable speaking and reading in English.

If you are interested in participating, please e-mail Rebecca at:
rebecca.jeong@carleton.ca

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

Carleton UNIVERSITY
Canada's Capital University

Recruitment Email: Sample

Subject: Carleton University: A research study to explore characteristics of cybersecurity warning messages

Body text:

RE: Looking for volunteers (children 10 to 12 years old)

Dear (Name),

I am a Masters student at Carleton University, working under the supervision of Dr. Sonia Chiasson. We are looking for volunteers for a research study that explores different characteristics of cybersecurity warning messages to understand how children interpret them.

As a participant in this study, your child will complete sorting activities and answer some questions. The study will take approximately 1 hour.

We are looking for children between the ages of **10 to 12 years old**, comfortable speaking and reading in English.

Each participant will be rewarded for their time with $20 cash. If you are interested in participating, please e-mail Rebecca at: rebecca.jeong@carleton.ca

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

Sincerely,
Rebecca Jeong

Carleton UNIVERSITY
Canada's Capital University

Adult Recruitment Email: Sample

Subject: Carleton University: A research study to explore characteristics of cybersecurity warning messages

Body text:

RE: Looking for volunteers

Dear (Name),

I am a Masters student at Carleton University, working under the supervision of Dr. Sonia Chiasson. We are looking for volunteers for a research study that explores different characteristics of cybersecurity warning messages to understand how we interpret them.

As a participant in this study, you will complete sorting activities and answer some questions. The study will take approximately 1 hour.

We are looking for adult volunteers over **18 years old**, comfortable speaking and reading in English.

Each participant will be rewarded for their time with $20 cash. If you are interested in participating, please e-mail Rebecca at: rebecca.jeong@carleton.ca

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

Sincerely,
Rebecca Jeong

Appendix D

Consent Forms and Assent Script

Carleton UNIVERSITY
Canada's Capital University

Parental Consent Form for Children's Participation in Research

Title: Hazard matching: Iteratively designing effective cybersecurity and privacy warning messages for children

CUREB-B clearance #: 108364

Date of ethics clearance: January 11, 2018

Ethics Clearance for the Collection of Data Expires: January 31, 2019

Introduction

The purpose of this form is to provide you (as the parent/legal guardian of a prospective research study participant) with the information that may affect your decision to give consent for your child's participation in this research study. The researcher for this study is a Masters student, **Rebecca Jeong**. She is working under the supervision of Dr. Sonia Chiasson **in The School of Computer Science.** Read the information below and ask any questions you might have before making a decision. If you decide to let your child be involved in this study, this form will be used to record your permission.

Purpose of the Study

If you agree, your child will be asked to participate in a research study exploring different characteristics of cybersecurity warning messages to understand how children interpret them. The results from this study will be used to make recommendations in better designing effective warning messages.

What is my child going to be asked to do?

Your child will be asked to complete card sorting and ranking activities. This will allow us to understand how children perceive the severity of the hazard associated with various characteristics of cybersecurity warning messages (e.g., signal words, colours, symbols, or other similar characteristics). Please note that your child is not being tested; we are only interested in your child's perception of cybersecurity warning messages. This research study will be audio-recorded for the purposes of

transcription and analysis. The participants will not be photographed; photographs will only be taken of the sorted cards.

Today's session will take approximately 1 hour. It involves a pre-test questionnaire, sorting activities and a post-test interview. There are no foreseeable risks in participating in this study. Your child will not be asked to disclose any personally identifiable information. If such information is voluntarily disclosed, it will be discarded when transcribing the interview to text.

Eligibility

In order to participate in this study, your child must be between the ages of 10 to 12 years old and be comfortable speaking and reading in English.

Compensation

As a token of appreciation, your child will receive $20 cash for participating in this study. If the study takes place on campus such as the CHORUS lab, we will also reimburse parking costs if applicable at the end of the session.

Does my child have to participate?

No, your child's participation in this study is voluntary. In addition to your consent, your child must also agree to participate in the study. Your child may decline to participate or to withdraw from participation at any time during the session.

If your child does not want to participate, they will not be included in the study and there will be no penalty. Your child will receive the $20 cash compensation even if they choose to withdraw from the study.

How will my child's privacy and confidentiality be protected?

Your child's privacy and the confidentiality will be protected. We encourage you to be nearby but not directly sitting with your child during the session. All responses will be kept anonymous. All research data and notes will be stored and retained on password protected computers or storage devices of the researchers for use in future research and the consent form will be kept in a locked cabinet. Access will be restricted only to the research team. Some of the questionnaires are hosted by Qualtrics. The data will be stored and protected by Qualtrics but may be disclosed via a court order data breach. Once the research is completed, audio recordings will be securely destroyed.

What if I do not want my child to be audio-recorded?

If you choose to not have your child audio-recorded, they may still participate in the study. The researcher will take notes of what the child said during the study.

The ethics protocol for this research was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

Researcher contact information:
Rebecca Jeong, Master's Student
School of Computer Science
Carleton University
Email: rebecca.jeong@carleton.ca

Supervisor contact information:
Dr. Sonia Chiasson
School of Computer Science
Carleton University
Tel: (613) 520-2600 ext. 1656
Email: chiasson@scs.carleton.ca

I, _____, give permission to my child, _____, to participate in this study on exploring cybersecurity and privacy warning messages.

_____ I consent to my child being audio-recorded for the purposes of transcription.

_____ _____
Signature of parent/legal guardian Date

_____ _____
Signature of a researcher Date

Carleton UNIVERSITY
Canada's Capital University

Assent (Verbal Consent) Script for Children

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 108364.

Hi, my name is Rebecca Jeong, a student at Carleton University. I need your help in organizing different characteristics of cybersecurity warning messages. I would like to see how dangerous or not dangerous you think the words, colours, and symbols I show you today. First, I will ask you some questions and then you will sort some cards.

After finishing the sorting activities, I will ask you some more questions and then we will be done. Today's session will take about 1 hour and I will record your voice so that I can remember your comments. If you don't want me to record your voice, please let me know. Also, I will take some photos of the sorted cards. Don't worry, I will not take any photos of you.

The information you will share with me will be safely locked up. No one will hear what you said except the people doing the research. Just remember, we are not testing you, we just want to hear your opinion.

You have the choice to join this study or not, it is entirely up to you. You can say okay now and change your mind later. All you have to do is tell me that you want to stop. Don't worry, no one will be hurt or get mad. Just let me know.

To thank you for your help, I will give you $20 cash. You can keep the money even if you decide to stop the study.

Do you have any questions? Remember that you can ask questions at any time.

Do you agree to participate in this user study and play the game?

- If yes, please say: yes, I will be in this research study
- If no, please say: no, I don't want to do this

Carleton UNIVERSITY
Canada's Capital University

Adult Participant Consent Form

Title: Hazard matching: Iteratively designing effective cybersecurity and privacy warning messages for children

CUREB-B clearance #: 108364

Date of ethics clearance: March 26, 2018

Ethics Clearance for the Collection of Data Expires: January 31, 2019

Introduction

The purpose of this form is to provide you with the information that may affect your decision to participate in this research study. The researcher for this study is a Masters student, **Rebecca Jeong**. She is working under the supervision of Dr. Sonia Chiasson **in The School of Computer Science.** Read the information below and ask any questions you might have before making a decision.

Purpose of the Study

If you agree, you will be asked to participate in a research study exploring different characteristics of cybersecurity warning messages to understand how adults interpret them in comparison to children. The results from this study will be used to make recommendations in better designing effective warning messages.

What am I going to be asked to do?

You will be asked to complete card sorting and ranking activities. This will allow us to understand how you perceive the severity of the hazard associated with various characteristics of cybersecurity warning messages (e.g., signal words, colours, symbols, or other similar characteristics). Please note that you are not being tested; we are only interested in your perception of cybersecurity warning messages. This research study will be audio-recorded for the purposes of transcription and analysis. The participants will not be photographed; photographs will only be taken of the sorted cards.

Today's session will take approximately 1 hour. It involves a pre-test questionnaire, sorting activities and a post-test interview. There are no foreseeable risks in participating in this study. You will not be asked to disclose any personally identifiable information. If such information is voluntarily disclosed, it will be discarded when transcribing the interview to text.

Eligibility

In order to participate in this study, you must be an adult over 18 years old and be comfortable speaking and reading in English.

Compensation

As a token of appreciation, you will receive $20 cash for participating in this study. If the study takes place on campus such as the CHORUS lab, we will also reimburse parking costs if applicable at the end of the session.

Do I have to participate?

No, your participation in this study is voluntary. You may decline to participate or to withdraw from participation at any time during the session.

If you do not want to participate, you will not be included in the study and there will be no penalty. You will receive the $20 cash compensation even if you choose to withdraw from the study.

How will my privacy and confidentiality be protected?

Your privacy and the confidentiality will be protected. All responses will be kept anonymous. All research data and notes will be stored and retained on password protected computers or storage devices of the researchers for use in future research and the consent form will be kept in a locked cabinet. Access will be restricted only to the research team. Some of the questionnaires are hosted by Qualtrics. The data will be stored and protected by Qualtrics but may be disclosed via a court order data breach. Once the research is completed, audio recordings will be securely destroyed.

What if I do not want to be audio-recorded?

If you choose to not be audio-recorded, you may still participate in the study. The researcher will take notes of what you said during the study.

The ethics protocol for this research was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

Researcher contact information:
Rebecca Jeong, Master's Student
School of Computer Science
Carleton University
Email: rebecca.jeong@carleton.ca

Supervisor contact information:
Dr. Sonia Chiasson
School of Computer Science
Carleton University
Tel: (613) 520-2600 ext. 1656
Email: chiasson@scs.carleton.ca

I, _____, agree to participate in this study on exploring cybersecurity and privacy warning messages.

_____ I consent to being audio-recorded for the purposes of transcription.

_____ _____
Signature of participant Date

_____ _____
Signature of a researcher Date

Appendix E

Questionnaires and Interview Script

Carleton UNIVERSITY
Canada's Capital University

Pre-test Questionnaire*

Participant ID (assigned):

Demographic Information

Q1) What is your age and what grade are you in?

Age: Grade: Prefer not to answer:

Q2) I am a:

❍ Male ❍ Female ❍ Other ❍ Prefer not to answer

Online and Electronic Device Usage Information

Q1) About how many days a week in general are you online?

Day(s):
Other, please explain (e.g., once/month):

Q2) Which of the electronic device(s) do you use to go online? (You may choose more than one option)

☐ Desktop computer
☐ Laptop computer (e.g., Apple, Windows, Chrome laptops)
☐ iPhone (Apple)
☐ Android phone (e.g., Samsung)
☐ Windows phone
☐ Blackberry
☐ iPad (Apple)
☐ Other tablets (e.g., Android, Chrome, Amazon Kindle, Kobo)
☐ Gaming consoles (e.g., X-box, Playstation, Nintendo)

* This questionnaire will be completed verbally and the researcher will audio-record the participant's responses and enter them into Qualtrics.

Questions specific to adult participants

Demographic Information

Q1) What is your age?

Age: Prefer not to answer:

Q3) What is the highest level of education you have completed? If currently enrolled, what level are you in?

- ☐ No schooling completed
- ☐ Nursery school to 8th grade
- ☐ Some high school, no diploma
- ☐ High school graduate, diploma or the equivalent (e.g., GED)
- ☐ Trade/technical/vocational training
- ☐ Some college credit, no diploma
- ☐ College diploma
- ☐ Bachelor's degree (e.g., BA, BSc, BCS, BID)
- ☐ Master's degree (e.g., MA, MSc, MCS, MDes)
- ☐ Professional degree (e.g., MD, DDS, DVM)
- ☐ Doctorate degree (e.g., PhD)
- ☐ Other
- ☐ Prefer not to answer

Q4) What is your current employment status?

- ☐ Employed full time (e.g., 30 or more hours per week)
- ☐ Employed part time (e.g., up to 29 hours per week)
- ☐ Unemployed and currently looking for work
- ☐ Unemployed and not currently looking for work
- ☐ Student
- ☐ Retired
- ☐ Self-employed
- ☐ Other
- ☐ Prefer not to answer

Q5) What is your program of study/current occupation?

* This questionnaire will be completed verbally and the researcher will audio-record the participant's responses and enter them into Qualtrics.

Carleton UNIVERSITY
Canada's Capital University

Post-test Semi-structured Interview*

These are some of the sample questions for the semi-structured interview.

Participant ID (assigned):

Characteristics of Cybersecurity Warning Messages

Q1) Did you have any trouble categorizing any of the colours? Please explain.

Q2) Did you have any trouble categorizing any of the words? Please explain.

Q3) Did you have any trouble categorizing any of the symbols? Please explain.

Previous Experience with Cybersecurity Warning Messages

Q3) What is a cybersecurity warning message (in your own words)? Please explain.

Q4) In your opinion, do you think having cyber security warning messages are positive, negative or both? Please explain.

Q5) What do you normally do online? What kind of activities (e.g., apps, social networking platforms, games, etc.)? Please explain.

Q6) Tell me about a time when you saw a cybersecurity warning message (story).

* This interview will be completed verbally and the researcher will audio-record the participant's responses and enter them into Qualtrics.

Q7) What do you do when you see warning messages? Please explain.

Q8) Have you shown warning messages to anyone else (e.g., parents, teachers, friends, etc.)? Please explain.

Q9) What would you expect to see on the cybersecurity warning message so that you know something dangerous is happening (e.g., colours, symbols, words)? Please explain.

* This interview will be completed verbally and the researcher will audio-record the participant's responses and enter them into Qualtrics.

Appendix F

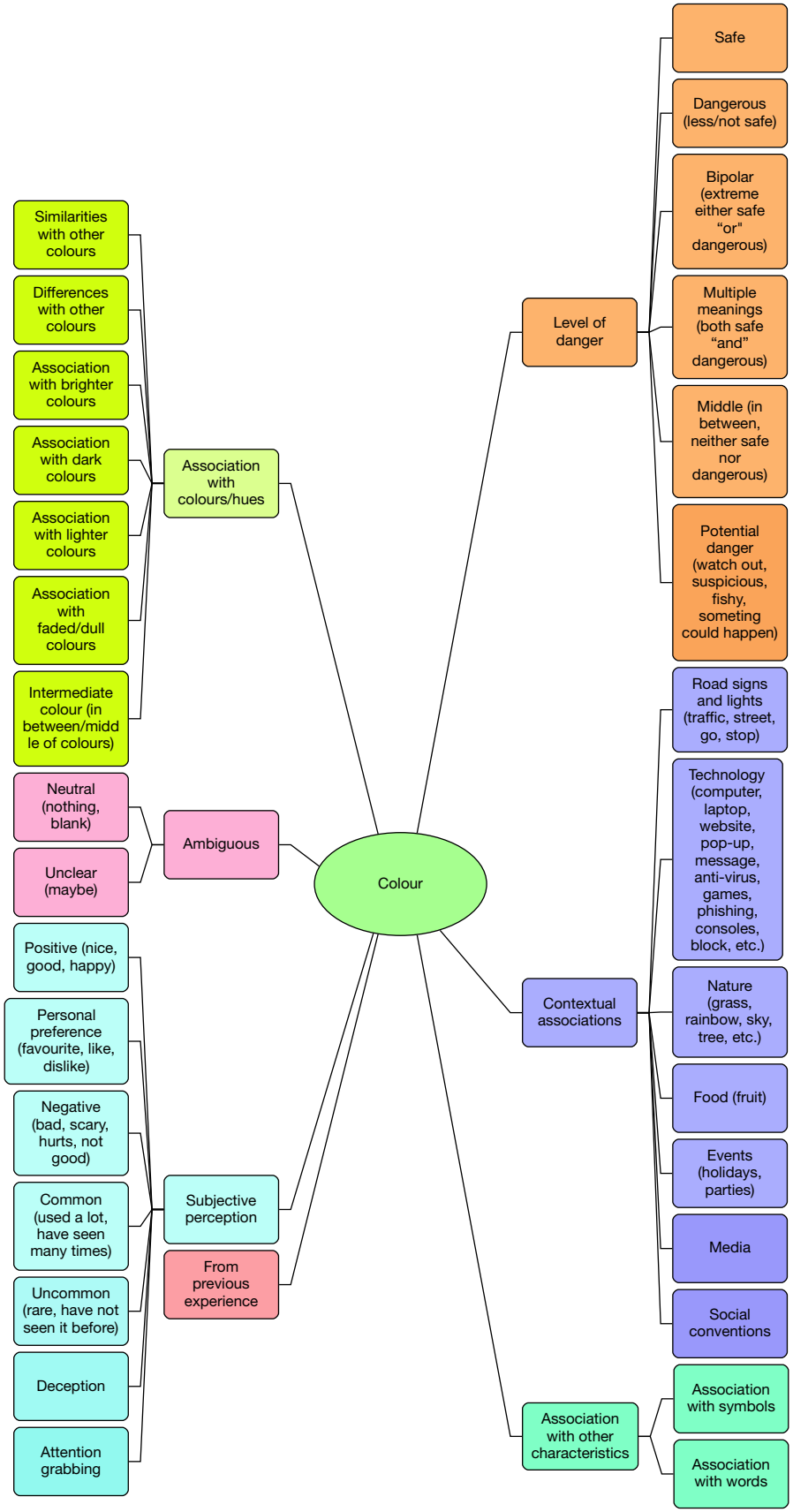
Qualitative Content Analysis Themes

F.1 Themes

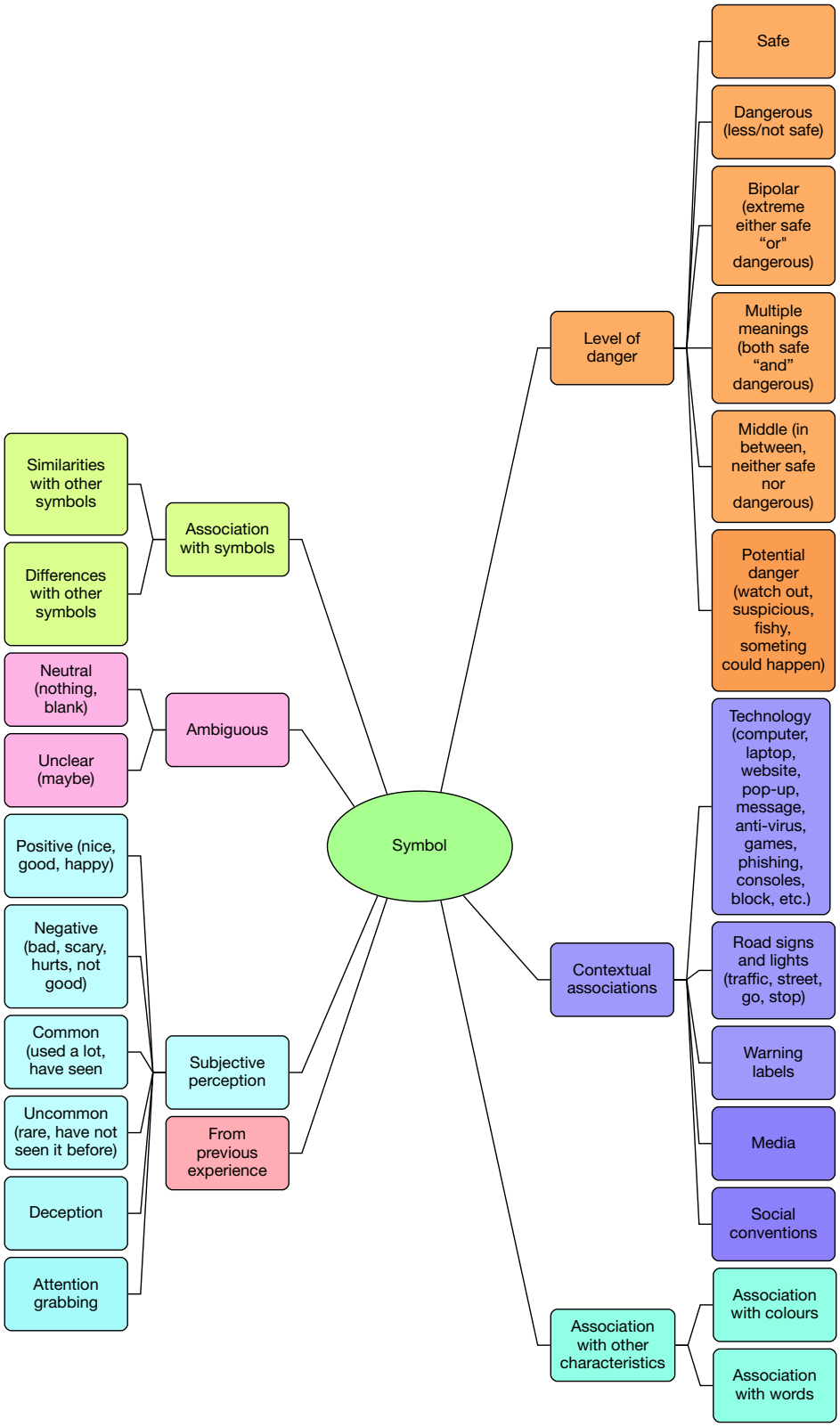
THEME	COLOUR SUBTHEME	SYMBOL SUBTHEME	WORD SUBTHEME
Level of danger	Safe Middle Dangerous Bipolar Multiple meanings Potential danger	Safe Middle Dangerous Bipolar Multiple meanings Potential danger	Safe Middle Dangerous Bipolar Multiple meanings Potential danger
Association with same parameters	Similarities with other colours Differences with other colours Intermediate colour (in between) Association with brighter colours Association with dark colours Association with faded/dull colours Association with lighter colours	Similarities with other symbols Differences with other symbols	Similarities with other words (synonyms) Differences with other words (antonyms)
Association with other parameters	Association with symbols Association with words	Association with colours Association with words	Association with colours Association with symbols
Contextual associations	Technology Events Food Media Nature Road signs and lights Social conventions	Technology Media Road signs and lights Social conventions Warning labels	Technology Media Social conventions
Subjective perception	Positive Negative Common Uncommon Attention grabbing Deception Personal preference	Positive Negative Common Uncommon Attention grabbing Deception	Positive Negative Common Uncommon Attention grabbing Deception
Ambiguous	Neutral Unclear	Neutral Unclear	Neutral Unclear
From previous experience			

F.2 Thematic Mind Maps

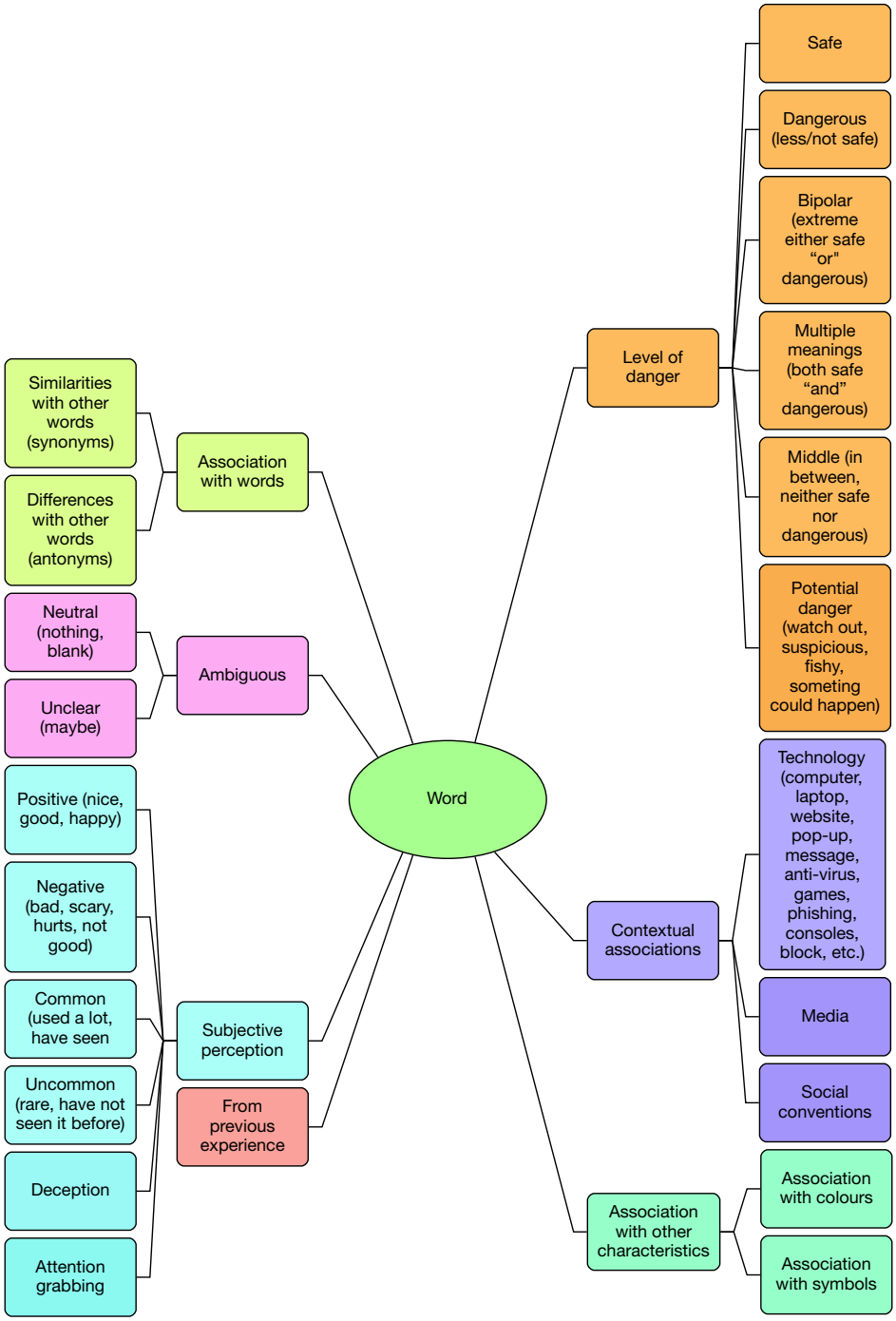
F.2.1 Colour Mind Map


Colour
Level of danger
Safe
Dangerous (less/not safe)
Bipolar (extreme either safe "or" dangerous)
Multiple meanings (both safe "and" dangerous)
Middle (in between, neither safe nor dangerous)
Potential danger (watch out, suspicious, fishy, someting could happen)
Contextual associations
Road signs and lights (traffic, street, go, stop)
Technology (computer, laptop, website, pop-up, message, anti-virus, games, phishing, consoles, block, etc.)
Nature (grass, rainbow, sky, tree, etc.)
Food (fruit)
Events (holidays, parties)
Media
Social conventions
Association with other characteristics
Association with symbols
Association with words
Association with colours/hues
Similarities with other colours
Differences with other colours
Association with brighter colours
Association with dark colours
Association with lighter colours
Association with faded/dull colours
Intermediate colour (in between/middle of colours)
Ambiguous
Neutral (nothing, blank)
Unclear (maybe)
Subjective perception
Positive (nice, good, happy)
Personal preference (favourite, like, dislike)
Negative (bad, scary, hurts, not good)
Common (used a lot, have seen many times)
Uncommon (rare, have not seen it before)
Deception
Attention grabbing
From previous experience

F.2.2 Symbol Mind Map


Symbol
Level of danger
Safe
Dangerous (less/not safe)
Bipolar (extreme either safe “or" dangerous)
Multiple meanings (both safe “and” dangerous)
Middle (in between, neither safe nor dangerous)
Potential danger (watch out, suspicious, fishy, someting could happen)
Contextual associations
Technology (computer, laptop, website, pop-up, message, anti-virus, games, phishing, consoles, block, etc.)
Road signs and lights (traffic, street, go, stop)
Warning labels
Media
Social conventions
Association with other characteristics
Association with colours
Association with words
Association with symbols
Similarities with other symbols
Differences with other symbols
Ambiguous
Neutral (nothing, blank)
Unclear (maybe)
Subjective perception
Positive (nice, good, happy)
Negative (bad, scary, hurts, not good)
Common (used a lot, have seen
Uncommon (rare, have not seen it before)
Deception
Attention grabbing
From previous experience

F.2.3 Word Mind Map


Word
Level of danger
Safe
Dangerous (less/not safe)
Bipolar (extreme either safe “or” dangerous)
Multiple meanings (both safe “and” dangerous)
Middle (in between, neither safe nor dangerous)
Potential danger (watch out, suspicious, fishy, someting could happen)
Contextual associations
Technology (computer, laptop, website, pop-up, message, anti-virus, games, phishing, consoles, block, etc.)
Media
Social conventions
Association with other characteristics
Association with colours
Association with symbols
Association with words
Similarities with other words (synonyms)
Differences with other words (antonyms)
Ambiguous
Neutral (nothing, blank)
Unclear (maybe)
Subjective perception
From previous experience
Positive (nice, good, happy)
Negative (bad, scary, hurts, not good)
Common (used a lot, have seen
Uncommon (rare, have not seen it before)
Deception
Attention grabbing

Appendix G

Quantitative Card Sorting and Ranking Visualization

G.1 Children's Sorting and Ranking Visualization

G.1.1 Signal Colours

G.1.2 Signal Symbols

G.1.3 Signal Words

		Colour																			
		Green	Cyan	Lime	Mint	Lavender	White	Pink	Blue	Coral	Purple	Olive	Magenta	Yellow	Brown	Navy	Grey	Orange	Maroon	Black	Red
Participants	1	1	8	2	7	5	6	3	10	4	9	13	12	14	16	19	17	15	18	11	20
	2	1	6	2	4	9	5	12	7	11	8	3	17	18	15	10	14	19	13	16	20
	3	11	3	7	10	6	9	2	4	14	5	12	1	8	13	17	15	16	18	19	20
	4	15	4	5	3	2	1	6	11	9	10	12	8	18	13	16	17	7	19	14	20
	5	9	14	13	4	5	7	8	16	1	17	10	15	18	6	12	2	3	11	20	19
	6	1	2	7	11	5	6	9	3	10	4	15	12	13	16	8	14	17	18	20	19
	7	1	7	2	4	5	10	6	9	13	12	3	11	16	14	8	18	15	17	20	19
	8	1	5	3	4	9	2	8	10	7	11	6	12	13	15	16	18	14	17	19	20
	9	8	7	3	6	5	1	4	9	2	12	14	13	10	18	15	16	11	19	17	20
	10	1	3	15	5	8	2	7	4	6	9	12	14	16	11	18	13	10	17	19	20
	11	5	2	11	1	4	9	12	3	10	15	6	18	16	14	7	13	17	19	8	20
	12	1	3	2	5	4	8	6	20	17	14	10	7	12	9	16	11	13	15	18	19
	13	7	2	14	11	9	1	6	5	12	3	8	4	13	16	17	10	18	15	19	20
	14	1	5	2	6	4	11	8	7	13	16	3	18	15	12	14	10	17	19	9	20
	15	1	4	2	7	13	5	6	3	14	15	11	12	8	10	17	18	9	16	19	20
	16	2	4	5	3	10	1	9	6	8	13	11	17	14	12	7	16	15	18	19	20
	17	7	4	5	1	2	18	3	9	12	10	13	11	6	14	17	15	8	16	19	20
	18	2	4	1	3	7	15	5	12	6	10	8	9	16	14	13	11	17	18	19	20
	19	1	6	2	7	10	8	9	3	15	11	5	18	16	13	4	12	17	19	14	20
	20	1	8	9	3	7	5	6	11	2	10	13	16	17	12	14	15	4	19	18	20
	21	1	2	9	10	4	14	12	3	11	5	15	13	8	16	7	6	17	19	18	20
	22	13	6	2	5	3	1	11	12	4	8	10	14	7	16	17	19	9	15	20	18
	Mean	4.136364	4.954545	5.590909	5.454545	6.181818	6.590909	7.181818	8.045455	9.136364	10.31818	9.681818	12.36364	13.27273	13.40909	13.13636	13.63636	13.09091	17.04545	17.04545	19.72727
	Median	1	4	4	5	5	6	6.5	8	10	10	10.5	12.5	14	14	14.5	14.5	15	18	19	20
	Mode	1	4	2	4	5	1	6	3	4	10	13	12	16	16	17	15	17	19	19	20
	Standard d	4.507089	2.785631	4.4149	2.955661	2.889	4.924759	2.938032	4.58234	4.601195	3.859267	3.883866	4.50973	3.844375	2.754375	4.485909	4.15813	4.709758	2.170742	3.592019	0.550482

		Symbol																			
		Happy face	Closed lock	Ticer/Secur	Circle?	Shield?	Triangle?	Key	Stop hand	Sad face	Circle!	Angry face	Triangle!	Shield!	Open lock	CircleX	ShieldX	TriangleX	Fire	Bug	and crossb
Participants	1	2	1	10	6	8	7	3	4	5	12	11	14	13	15	17	18	16	9	20	19
	2	1	2	3	5	6	7	9	4	18	11	8	12	13	19	14	17	15	10	16	20
	3	1	7	3	5	6	4	2	13	12	10	19	11	9	8	15	14	16	18	17	20
	4	1	2	3	7	6	8	9	4	10	13	12	15	14	11	16	17	18	20	5	19
	5	1	7	17	3	5	4	10	18	6	8	9	12	13	14	2	16	11	19	15	20
	6	3	2	1	9	7	11	4	13	6	10	14	18	8	5	15	17	16	19	12	20
	7	3	2	1	5	10	6	18	9	14	16	8	17	13	19	11	15	12	4	7	20
	8	1	4	2	12	9	13	3	5	6	15	11	14	10	7	17	18	16	8	20	19
	9	1	9	2	4	15	12	8	6	7	3	17	11	16	10	5	14	13	18	19	20
	10	2	3	1	6	8	7	4	5	14	9	13	10	11	12	15	16	17	19	18	20
	11	1	17	4	5	6	7	16	8	2	13	3	15	14	18	10	11	12	9	20	19
	12	2	1	3	4	9	7	11	6	12	5	14	8	10	19	15	18	13	16	17	20
	13	3	18	19	15	12	14	1	5	9	6	10	8	7	2	13	11	16	17	4	20
	14	1	3	16	4	6	5	2	8	18	9	17	10	13	15	11	14	12	7	19	20
	15	2	18	20	3	5	4	6	8	10	14	7	15	11	1	16	12	17	13	19	9
	16	1	10	9	12	14	13	3	8	4	5	11	6	7	2	15	17	16	18	19	20
	17	2	1	20	8	6	7	15	14	9	4	10	5	3	18	11	13	12	17	16	19
	18	1	13	11	5	7	8	10	6	2	15	3	14	17	4	9	12	16	18	19	20
	19	3	1	10	5	6	7	2	8	9	15	4	20	18	13	11	14	12	17	19	16
	20	1	5	4	12	8	10	7	3	2	13	14	11	9	6	17	15	16	18	19	20
	21	1	2	4	3	5	8	9	11	12	6	17	7	13	18	14	16	15	19	10	20
	22	1	2	19	4	6	5	20	13	7	3	10	9	8	16	14	11	12	15	17	18
	Mean	1.590909	5.909091	8.272727	6.454545	7.727273	7.909091	7.818182	8.136364	8.818182	9.772727	11	11.90909	11.36364	11.45455	12.86364	14.81818	14.5	14.90909	15.77273	19
	Median	1	3	4	5	6.5	7	7.5	8	9	10	11	11.5	12	12.5	14	15	15.5	17	17.5	20
	Mode	1	2	3	5	6	7	3	8	12	13	11	14	13	19	15	17	16	18	19	20
	Standard d	0.796366	5.789227	7.099174	3.432718	2.814619	3.022284	5.543219	3.979656	4.696872	4.253086	4.482771	3.938928	3.606152	6.185446	3.870468	2.383202	2.154729	4.789961	4.956303	2.429972

		Word																			
		Protect	Security	Online	Message	Notice	Careful	Important	Don't	Blocked	Attention	Suspicious	Alert	Warning	Error	Urgent	Unsafe	Damage	Virus	Hack	Fatal
Participants	1	2	6	1	5	9	8	12	4	3	17	7	10	16	11	13	14	15	19	20	18
	2	1	2	4	3	5	9	8	17	6	13	16	12	14	7	15	18	10	11	19	20
	3	2	1	6	7	8	5	9	13	12	3	16	4	14	11	10	15	19	18	17	20
	4	1	4	7	6	8	2	5	9	14	10	11	3	12	15	13	17	19	18	16	20
	5	8	2	1	3	6	5	17	9	4	13	7	12	10	14	16	20	11	18	19	15
	6	2	1	9	3	4	6	11	13	14	7	5	16	10	8	15	19	17	12	18	20
	7	2	1	4	10	11	3	5	7	8	16	13	14	17	12	6	9	15	19	20	18
	8	2	1	4	3	8	5	9	7	13	6	10	11	12	15	17	14	16	20	19	18
	9	1	3	5	6	4	2	8	7	14	10	13	12	11	9	15	16	17	18	19	20
	10	2	1	15	9	4	6	8	5	7	11	14	3	12	10	16	19	13	17	18	20
	11	1	15	2	3	10	5	4	9	13	8	6	11	19	14	20	7	16	18	17	12
	12	1	4	3	11	8	10	5	9	2	13	6	15	7	18	19	12	14	16	17	20
	13	2	1	8	3	5	9	6	7	19	4	10	11	14	15	13	17	12	20	16	18
	14	1	2	3	5	4	10	6	7	8	11	15	13	16	12	9	17	14	18	20	19
	15	2	9	1	3	4	6	10	11	18	17	8	12	7	16	5	14	15	19	13	20
	16	10	14	2	1	3	7	5	9	6	4	11	13	12	19	15	8	18	17	16	20
	17	1	10	8	2	5	6	3	15	9	11	12	4	13	19	7	14	16	17	18	20
	18	2	16	4	3	1	6	8	5	10	9	11	7	15	12	14	13	17	19	20	18
	19	1	3	4	6	5	11	8	9	2	7	12	13	14	15	10	17	16	18	19	20
	20	3	4	9	5	8	2	6	14	1	12	7	18	17	13	11	19	10	16	15	20
	21	1	3	2	6	7	4	8	11	15	10	5	13	12	9	19	14	16	18	17	20
	22	16	5	6	15	1	17	7	14	13	4	8	2	10	12	3	11	9	19	18	20
	Mean	2.9090909	4.9090909	4.9090909	5.3636364	5.8181818	6.5454545	7.6363636	9.5909091	9.5909091	9.8181818	10.136364	10.409091	12.909091	13	12.772727	14.727273	14.772727	17.5	17.772727	18.909091
	Median	2	3	4	5	5	6	8	9	9.5	10	10.5	12	12.5	12.5	13.5	14.5	15.5	18	18	20
	Mode	2	1	4	3	8	6	8	9	14	13	7	12	12	15	15	14	16	18	19	20
	Standard d	3.7021112	4.7899606	3.4074022	3.3742083	2.7016109	3.5149649	3.0790452	3.5140411	5.2974306	4.1591707	3.50911	4.5529592	3.1000628	3.3665016	4.6693715	3.653854	2.8773635	2.2200386	1.8239627	1.9978343

G.2 Adults' Sorting and Ranking Visualization

G.2.1 Signal Colours

G.2.2 Signal Symbols

G.2.3 Signal Words

		Colour																			
		Green	Lime	Mint	Cyan	Lavender	Blue	Pink	White	Purple	Coral	Olive	Brown	Grey	Navy	Magenta	Black	Orange	Yellow	Maroon	Red
Participants	1	1	2	5	4	12	6	14	8	13	11	3	15	9	7	17	10	16	18	19	20
	2	2	9	8	4	6	3	7	1	11	5	13	12	15	14	10	16	18	19	17	20
	3	7	6	4	5	1	13	2	8	9	3	11	12	10	14	18	15	17	16	19	20
	4	7	17	3	4	2	6	1	13	10	12	11	5	15	9	14	8	19	18	16	20
	5	10	5	4	6	2	9	1	12	7	3	14	15	13	16	8	19	11	17	18	20
	6	1	2	4	10	14	9	13	6	15	11	3	12	7	8	17	5	19	18	16	20
	7	1	2	6	9	3	8	4	5	13	10	7	11	12	14	16	20	18	15	17	19
	8	1	9	16	10	6	4	14	2	11	17	12	7	13	18	19	3	8	15	5	20
	9	4	5	3	1	7	2	10	9	12	8	6	11	14	13	16	15	18	19	17	20
	10	3	1	11	2	6	4	5	9	7	12	13	14	10	15	8	16	19	18	17	20
	11	14	7	4	15	2	16	3	9	5	1	13	12	10	17	6	20	8	11	19	18
	12	1	2	3	4	5	10	6	9	15	14	11	13	17	18	7	19	16	8	12	20
	13	3	4	5	2	7	1	6	10	8	9	12	13	11	14	17	18	16	15	19	20
	14	1	9	10	3	5	2	13	11	4	17	15	14	16	6	7	12	8	18	19	20
	15	1	2	3	5	9	6	10	8	12	11	4	15	16	7	18	17	14	13	19	20
	16	11	13	4	6	2	7	3	1	8	5	16	10	9	12	18	19	15	14	17	20
	17	1	2	7	5	11	4	8	3	12	15	9	13	14	6	17	10	18	16	19	20
	18	1	2	5	6	3	7	4	15	8	10	14	12	11	13	9	16	17	18	19	20
	19	8	7	4	12	3	13	2	1	6	5	11	10	16	14	9	20	17	15	18	19
	20	1	2	5	6	4	7	3	13	9	8	10	12	14	11	16	15	19	18	17	20
	21	2	5	6	4	11	1	14	8	12	15	7	16	9	3	13	10	18	19	17	20
	22	2	1	5	3	9	6	16	7	10	15	4	11	8	13	12	20	14	17	18	19
	Mean	3.772727	5.181818	5.681818	5.727273	5.909091	6.545455	7.227273	7.636364	9.863636	9.863636	9.954545	12.04545	12.22727	11.90909	13.27273	14.68182	15.59091	16.13636	17	19.77273
	Median	2	4.5	5	5	5.5	6	6	8	10	10.5	11	12	12.5	13	15	16	17	17	17.5	20
	Mode	1	2	4	4	2	6	14	8	12	11	11	12	9	14	17	20	18	18	19	20
	Standard d	3.914951	4.193378	3.153024	3.480309	3.727748	3.996752	4.93705	4.08884	3.044049	4.693414	4.005678	2.57233	2.975004	4.219107	4.442027	5.06516	3.660069	2.782521	3.132016	0.528413

	Symbol																			
	Happy face	Key	Closed lock	Open lock	Circle?	Triangle?	Shield?	Circle!	Sad face	Shield!	icer/Secur	Stop hand	Triangle!	TriangleX	CircleX	ShieldX	Angry face	Bug	Fire	and crossb
1	15	5	9	18	2	11	3	6	16	8	19	14	12	13	4	10	17	1	7	20
2	2	1	3	4	8	10	9	15	6	16	18	5	17	13	11	12	7	14	20	19
3	1	4	8	7	14	11	9	15	13	10	20	19	12	16	17	2	18	5	3	6
4	1	5	3	4	7	8	6	11	13	10	2	14	12	18	17	16	15	9	19	20
5	1	7	3	2	12	13	10	9	4	8	6	5	11	14	15	16	17	19	18	20
6	3	2	1	4	6	7	8	9	12	11	17	5	10	15	14	16	13	19	18	20
7	2	3	1	4	5	6	7	13	12	17	10	11	15	16	14	18	8	19	9	20
8	1	3	2	17	15	16	10	7	8	5	14	9	6	13	11	12	4	18	19	20
9	2	4	3	5	11	12	10	14	17	13	1	20	15	9	7	8	18	19	6	16
10	1	2	15	3	9	8	7	6	10	4	17	18	5	12	13	11	16	14	19	20
11	1	3	6	7	4	8	5	11	13	9	12	2	10	14	19	17	15	20	16	18
12	1	4	2	15	5	6	10	9	7	11	18	3	12	14	8	13	16	17	19	20
13	1	3	4	5	10	9	8	11	7	15	2	18	12	13	14	16	17	6	19	20
14	1	7	4	5	2	13	9	15	8	10	6	3	16	14	12	11	19	18	17	20
15	4	2	1	18	5	6	7	8	11	10	3	16	9	13	14	12	15	17	19	20
16	1	4	2	3	10	8	13	12	7	16	5	17	11	9	18	15	6	20	14	19
17	2	3	1	11	7	8	6	10	12	9	4	5	13	16	15	14	17	19	18	20
18	1	2	9	8	5	6	11	4	13	12	3	7	10	18	20	19	14	15	17	16
19	1	4	2	5	8	11	14	9	6	15	3	7	12	13	10	16	18	17	19	20
20	1	3	2	11	10	8	7	5	12	6	15	14	17	18	16	9	13	4	19	20
21	1	3	2	4	5	9	15	6	8	16	12	14	10	11	7	17	13	18	19	20
22	2	5	3	4	1	10	11	14	6	17	16	12	18	8	13	19	7	15	9	20
Mean	2.090909	3.590909	3.909091	7.454545	7.318182	9.272727	8.863636	9.954545	10.04545	11.27273	10.13636	10.81818	12.04545	13.63636	13.13636	13.59091	13.77273	14.68182	15.59091	18.81818
Median	1	3	3	5	7	8.5	9	9.5	10.5	10.5	11	11.5	12	13.5	14	14.5	15	17	18	20
Mode	1	3	2	4	5	8	10	9	13	10	3	14	12	13	14	16	17	19	19	20
Standard d	2.990606	1.532477	3.490246	5.17068	3.784509	2.657995	2.899843	3.443106	3.525111	3.91799	6.692536	5.892985	3.330627	2.786796	4.132282	4.101789	4.47141	5.784926	5.160833	3.111214

		Word																			
		Online	Message	Protect	Notice	Security	Attention	Important	Careful	Alert	Don't	Blocked	Error	Warning	Urgent	Unsafe	Suspicious	Damage	Hack	Virus	Fatal
Participants	1	2	1	8	3	4	5	7	9	6	10	16	11	13	12	14	15	19	18	20	17
	2	1	2	6	5	11	4	8	9	10	7	3	14	13	12	17	15	18	19	16	20
	3	2	1	5	13	6	3	7	4	11	20	10	14	15	9	8	17	19	12	16	18
	4	3	4	1	5	2	6	9	8	10	11	13	17	7	15	14	12	16	19	18	20
	5	2	1	6	5	14	3	4	7	12	15	16	11	9	13	8	10	18	19	17	20
	6	4	1	10	2	9	3	7	12	5	11	13	6	14	8	16	15	17	18	19	20
	7	3	4	1	6	2	7	9	8	10	5	15	12	14	11	16	18	17	19	20	13
	8	3	1	7	4	14	11	8	6	5	2	17	10	13	9	12	15	19	20	18	16
	9	3	4	1	8	2	14	13	9	10	5	6	7	16	15	12	11	17	18	19	20
	10	2	3	1	7	5	15	14	10	8	12	4	6	11	19	16	9	17	18	13	20
	11	1	2	3	7	10	4	5	8	17	9	6	13	11	16	15	12	14	18	19	20
	12	8	1	4	2	7	10	3	9	5	20	11	13	12	14	6	15	18	17	16	19
	13	4	3	1	7	6	8	2	5	11	9	13	17	15	12	10	14	16	18	19	20
	14	1	3	11	2	10	4	6	5	7	12	9	15	13	14	8	16	17	20	19	18
	15	3	4	1	5	2	8	13	9	7	17	12	11	6	14	19	10	18	16	15	20
	16	2	3	1	10	6	16	14	4	17	5	8	11	15	12	9	7	18	13	19	20
	17	2	3	4	5	1	9	7	6	8	13	11	16	12	10	15	14	19	17	18	20
	18	2	1	16	3	6	5	12	4	8	7	10	11	14	15	13	19	9	17	18	20
	19	3	4	1	6	2	7	5	9	11	8	15	12	14	17	13	10	16	19	18	20
	20	1	3	5	2	4	8	7	6	15	10	12	13	9	11	18	14	17	16	19	20
	21	2	3	1	4	12	7	6	5	8	11	13	9	10	14	15	16	17	18	19	20
	22	1	4	3	5	2	12	11	6	10	7	9	14	8	13	20	19	16	17	18	15
	Mean	2.5	2.545455	4.409091	5.272727	6.227273	7.681818	8.045455	7.181818	9.590909	10.27273	11	11.95455	12	12.95455	13.36364	13.77273	16.90909	17.54545	17.86364	18.90909
	Median	2	3	3.5	5	6	7	7	7.5	10	10	11.5	12	13	13	14	14.5	17	18	18	20
	Mode	2	1	1	5	2	4	7	9	10	7	13	11	13	12	8	15	17	18	19	20
	Standard d	1.535299	1.223861	4.043326	2.728715	4.139609	3.932603	3.49799	2.2176	3.459412	4.702399	3.891382	3.124058	2.794553	2.716392	3.873542	3.279544	2.158242	1.969464	1.726418	1.973855