MULTIMEDIA APPROACHES FOR IMPROVING CHILDREN'S PRIVACY AND SECURITY KNOWLEDGE AND PERSUADING BEHAVIOUR CHANGE

by
Leah Zhang-Kennedy

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

DOCTOR OF PHILOSOPHY

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2017

© Copyright by Leah Zhang-Kennedy, 2017

Abstract

By grades 4 to 11, 98% of Canadian children have Internet access outside of school. Computer security and privacy technology reduces children's online risks, but the success of such technology is also dependent on individuals' behaviour that could be improved through education and training. We studied the effects of multimedia educational tools on children's privacy and security knowledge and behaviour. Our qualitative study of children's privacy perceptions showed that they have a poor understanding of privacy and security threats. Using design principles from persuasive technology and instructional design, we designed tools that teach children about privacy and security concepts. We created an online interactive comic and evaluated it with children 11 to 13 years old, and an interactive ebook for children 7 to 9 years old. Both user studies showed superior improvements in children's privacy knowledge, retention, and privacy-conscious behaviour compared to text-only formats. Children found these tools engaging, easy to use, and easy to learn. From these empirical findings, we find that multimedia educational tools create engagement, extend learning, and have the potential to influence children's behaviour in the longer term.

Acknowledgements

This journey has been an incredibly rewarding experience, thanks to the people who inspired, encouraged and supported me.

I sincerely express my gratitude to my supervisor, Sonia Chiasson, who provided tremendous guidance in my research, and aspired me to produce quality work that aimed at the eventual publication of my projects. Sonia helped me to become a better researcher, writer, communicator, and a more confident individual. Acquiring these skills was rewarding to me as a student, and invaluable throughout my career.

I thank the members of my thesis committee, Rilla Khaled, Hussein Al Osman, Kasia Muldner, and Robert Biddle for their expertise and feedback from diverse perspectives that greatly helped me to improve this dissertation. I am particularly grateful to Robert, who provided continuous mentorship throughout my degree. His advice and insights were always an inspiration.

I am thankful to the people at the School of Computer Science at Carleton University who embraced my multidisciplinary background and gave me the opportunity to pursue my area of research. Special thanks to my colleagues in the CHORUS and HotSoft research groups who have assisted with experiments, listened to presentations, and offered discussions and feedback throughout the process.

I thank my husband Matt, a mathematician who I dubbed my unofficial "graduate advisor" over the years, guided me on a number of academic decisions. His wit and dedication to research never fail to impress me.

I thank my parents, Zhijian and Charles, and my mother and father in-laws, Della and Brent, for their love and emotional support.

Lastly, the fruit of this research would not been possible without my participants, whose observations and insights contributed to the quality of the work. I am particularly indebted to the bright little girls and boys, whose spirited hearts reminded me to never lose our childish playfulness and enthusiasm to life and work.

Some of the research included in this thesis has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Online privacy and security are not only a technical problem, but are also significantly impacted by people who interact with online content. Users' online privacy and security are more likely to be jeopardized when users are unaware of the security vulnerabilities, misunderstand the risks, or underestimate their susceptibility, even when security mechanisms are set in place to protect users [182]. It is therefore necessary to improve users' overall privacy and security understanding so they can make informed decisions as opportunities arise.

Usable security focuses on the human aspects of computer security and studies "the usability of security tools and the process of designing secure systems for the real-work context in which they have to operate" [149]. Usable security, therefore, recognizes that knowledge of human factors and design principles help to produce security solutions that are effective in practice. Until recently, children had not been a central focus in the design of privacy and security solutions. The design of solutions used by children needs to consider changes in children's developmental needs, the frequent involvement of adults in children's interactions with technology (e.g., parents and teachers), the context of use, and differences in cultural and societal assumptions of what is good for children [138].

Access to mobile media devices has increased dramatically among children [143]. By grades 4 to 11, 98% of Canadian children had Internet access outside of school [166]. This upsurge in online activities has increased children's exposure to online privacy risks [143]. Although privacy enhancing software and parental supervision reduce children's privacy risks, they do not empower children to critically think about the impact of their online actions, or help them develop practical skills for maintaining online privacy and security in the absence of such oversight. To empower children to be responsible digital citizens, researchers (e.g., [154, 166]) advocate for child-friendly education initiatives to prepare children to navigate online situations that require informed decision-making.

Presently, we lack appropriate resources to teach young children about online privacy and security. Educational initiatives (e.g., work by MediaSmarts and the Office of the Privacy Commissioner of Canada) frequently focus on tweens, teens, and adults as their primary audience. Some educational material for children is available (e.g., [109–112]), but many have not been systematically evaluated for effectiveness. Children are still developing literacy and cognitive skills, and have limited experience, which pose constraints on educational content and format. Furthermore, persuading children to behave in a secure and private manner is difficult because, like adults, they typically do not regard privacy and security as primary concerns [182].

1.2 Research Statement

The goal of this research is to discover if multimedia educational tools for children have positive effects on their privacy and security knowledge and behaviour. We explore two types of multimedia formats for children: online interactive comics and interactive ebooks. The main research question is:

> Can multimedia approaches create effective, memorable, and persuasive tools for educating children about online privacy and security concepts?

The objectives of this research are:

Objective 1: Conceptualize a behaviour model that describes the main challenges of privacy and security behaviour change.

Objective 2: Explore and identify families' online perceptions and practices of privacy and security.

Objective 3: Design and develop multimedia tools for children using Persuasive Technology (PT) and Instructional Design (ID) principles.

Objective 4: Evaluate the multimedia tools for effectiveness at increasing children's privacy and security knowledge and behaviour.

1.3 Contributions

The main contributions of the research are:

1. We proposed the Behaviour Model of Privacy and Security (BMOPS) for understanding two major factors for influencing user behaviour, mental models and motivation. We highlighted differences between privacy and security, and suggested that educational tools should aim to improve users' mental models due to complexities in users' motivation affected by tradeoffs in privacy and security and individual differences.

2. We identified several research gaps in a literature review of existing privacy and security education work created for adults and children under persuasive technology (PT) and instructional design (ID) principles.

3. We identified four models of online privacy primarily based on physical privacy, and children and parents' child-adversary threat models from interviews with families about their online practices, perceived risks, and protection strategies. We found that children's concerns of online threats differed from the threats that parents perceived are faced by children, which could influence the protection strategies used by children, and by parents to protect children.

4. We designed and developed two prototypes for children based on PT and ID design principles. Secure Comics about mobile online privacy educated children about online tracking and geo-tagging, and the Cyberheroes interactive ebook educated younger children about online privacy. Both high-fidelity prototypes became free educational resources for the public to access online and in the Apple Store.

5. We evaluated Secure Comics with children 11 to 13 years old, and Cyberheroes with children 7 to 9 years old. Both prototypes showed superior learning effects in knowledge retention and sustainable behavioural effects based on situational scenarios compared to text-only formats.

6. We addressed the research gap that many existing privacy and security education work for children lacked formal evaluation. Our user studies provided rare empirical evidence of the effectiveness of multimedia educational tools for educating children about privacy and security.

7. We compared the learning outcomes of our prototypes and identified the PT and ID design principles that led to increased engagement and improvements in privacy and security knowledge, retention, and behaviour.

1.4 Related Publications

Significant portions of the research in this thesis have appeared or have been submitted to peer-reviewed academic venues. Zhang-Kennedy is the primary author of these publications and conducted the majority of the work. Co-authors include graduate student researchers (Christine Mekail, Yomna Abdelaziz, and Elias Fares) and an undergraduate student research assistant (Khadija Baig), who helped with data collection and analysis. A large portion of text from published work in this thesis is taken directly for the publications.

The peer-reviewed full-paper publications are:

- **L. Zhang-Kennedy**, S. Chiasson, and R. Biddle. [Journal Article] The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cyber Security. *International Journal of Human-Computer Interaction*, 32:215-257, 2016.

- **L. Zhang-Kennedy**, C. Mekhail, Y. Abdelaziz, and Sonia Chiasson. [Conference Paper] From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Interaction Design and Children (IDC)*. ACM, 2016.

- **L. Zhang-Kennedy**, E. Fares, S. Chiasson, and R. Biddle. [Conference Paper] The Effects of Interactivity on Information Visualization about Internet Phishing Trends. In *APWG eCrime*. IEEE, 2016.

The peer-reviewed poster publications and workshop papers are:

- **L. Zhang-Kennedy**, C. Mekhail, Y. Abdelaziz, and Sonia Chiasson. [Extended Abstract] Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge. In *Interaction Design and Children (IDC)*. ACM, 2016.

- **L. Zhang-Kennedy**, and S. Chiasson. [Workshop paper] Improving Children's Mobile Privacy Awareness and Behaviour. *Symposium on Usable Privacy and Security Workshop on Inclusive Privacy and Security (WIPS)*, 2015.

Full papers currently in submission are:

- **L. Zhang-Kennedy**, Y. Abdelaziz, S. Chiasson. [Journal Article] Cyberheroes: The Design and Evaluation of an Interactive Ebook to Educate Children about Online Privacy. *International Journal of Child-Computer Interaction (IJCCI)*, 2017. (In revision)

- **L. Zhang-Kennedy**, K. Baig, and S. Chiasson. [Conference Paper] Comics for Children's Online Privacy Education. *British HCI*. ACM, 2017. (Accepted)

1.5 Thesis Outline

This thesis is organized as follows: In Chapter 2, we give a background on children's developmental needs, and outline concerns for children's privacy and security. In Chapter 3, we propose a Behaviour Model of Privacy and Security to conceptualize positive behaviour based on two dimensions: motivation and mental models. This is followed by a literature review of existing educational tools for adults and children in Chapter 4, where we examine the design approaches used. Next, in Chapter 5, we describe the design of our work, Secure Comics, and report our findings with children

11 to 13 years old in Chapter 6. To gain a first-hand understanding of privacy and security issues from children's perspective, the research presented in Chapter 7 studied children's privacy models and threat perceptions. Chapter 8 describes an interactive ebook called Cyberheroes that we designed for younger children, and Chapter 9 reports the findings with children 7 to 9 years old. In Chapter 10, we discuss our experiences using the design principles and make conclusions about whether they are useful for designing children's educational tools.

Chapter 2

Children's Development and Considerations

Children have different developmental needs than adults, but they also share some similarities with adults in human factors affecting privacy and security decisions. This chapter provides a background on children's developmental differences and their implications for children's privacy and security Education.

Children clearly have different characteristics than adults, such as their physical sizes and abilities [122], memory and processing capabilities [44,130,132], and literacy skills [51], which should be taken into consideration in the design of children's technology. According to Read and Bekker [138], key differences between child-computer interaction and adult-computer interaction are the rate of change in children's developmental characteristics (cognitively and physically), the frequent involvement of adults in children's interactions with technology, and the underlying cultural and societal assumptions about technology and what is good for children.

2.1 Children's Cognitive Developmental Differences

Children have rapid developmental rates compared to the fairly stable developmental states of adults. Piaget [133] proposed that all children go through a series of developmental stages to attain logical, analytical, and scientific thinking. At each stage, children's interaction with technology is limited by their physical and mental capabilities. The provided age spans should be regarded with the acknowledgement that variability exists in children, and the stages may be different between individuals.

Sensory-Motor Stage, Ages 0-2: Infants use their sensory abilities (e.g., seeing, touching, hearing) to discover relationships between themselves and the environment. They start to develop concepts of causality, such as learning that an object (real or virtual) can be moved by a hand.

Pre-Operational Stage, Ages 2-7: Starting at age two, children develop an understanding that symbols are representations of something else [43]. For example, a visual symbol of a button on a computer screen is perceived by children as a button that can be pressed. In computer security, symbolic representation is commonly used to support mental models [87], such as the depiction of key and lock symbols in software and user interface design. Children may need to learn the meaning of these advanced symbols when encountering them for the first time.

Children at the pre-operational stage are capable of seeing the environment from their own perspective, but they have difficulty considering what they see from someone else's perspective [131,132]. Pre-school children also have difficulties reversing action in their head and rely mainly on qualitative characteristics to solve problems [57]. This is a major drawback in learning privacy and security concepts because users are often required to troubleshoot issues and navigate complex interfaces. These characteristics also make it challenging to partner with children at the pre-operational stage in the design of technologies [73].

Concrete Operational Stage, Ages 7-11: Children in the concrete operational stage are the main user group we explored in our research. Elementary school children have developed the skills for understanding symbolic representation. They are mentally capable to reverse simple actions in their head, and are capable of using quantitative measures to solve problems and to make decisions [57]. Children at the concrete operational stage are more likely to appreciate seeing things from others' perspective. This enables them to work better with other children and with adults. Limitations from this stage is that children have difficulties understanding hierarchies and use deductive reasoning; they tend to focus on only one characteristic at a time [130,132].

Formal Operational Stage, Ages 11-16: Children at the formal operational stage are more consistently capable of abstract and logical thinking. They have developed the ability to understand hierarchies, use deductive reasoning, and analyze options logically [130,132]. This age group is capable of using a greater variety of technologies and software than younger children [130].

2.2 Other Developmental Characteristics

Due to the limitations in children's developmental abilities in the pre-operational years, our research focuses on children in the concrete operational stage and early years of the formal operational stage. We describe other developmental characteristics of children 7 to 13 years old.

Motor skills: Children 11 to 13 years old are capable of using motor skills for reaching, pointing, tapping, and dragging objects on a touchscreen tablet. This involves an initial long movement for reaching so that the hand gets closer to the object to be manipulated, then followed by a series of smaller movements using fingers such as pointing and tapping. Research evidence [11] suggests that visual feedback supports these tasks by helping children adjust their movements. The speed to perform these motor tasks increases in early childhood and are comparable to adults by age 10 [122]. Children aged 11 to 13 are therefore have greater control over their fine motor skills than younger children and are more comfortable using precision input or pointing devices such as a mouse [27].

Literacy: Children have limited vocabulary and therefore, textual communication in children's technologies should avoid complex words and technical jargon. Most children, however, have developed the skills to spell common words by age 8 and can read primary-level books [171]. By age 13, children have developed strong reading and communication skills. They have a larger vocabulary and greater mastery of the language than younger children [171]. Druin et al. [51] suggest that the use of text should be minimized in the design of children's technologies to reduce their cognitive load, particularly for the younger children in our target age group who are just starting to read.

Memory: Memory is often described in short or long-term. Working memory stores information in the short term, which can be retrieved to coordinate perception, long-term memory, and action [8]. Adults can hold seven chunks of information at a time [118], whereas five-year-old children can typically hold up to four or five chunks, and nine-year-olds up to six chunks [44]. The implication of younger children's limited working memory on technology design is that they hold less information when problem solving. This limits their capability to establish relationships between complex pieces of information. Experience plays a role in the efficient use of working memory, and therefore, provides older children with strategies that can be used to improve their performance, such as chunking information [57].

Long-term memory retrieves information by consciously recalling previous experiences or known facts. Long-term memory is also age-correlated because having more previous knowledge about the information to be encoded leads to improved memorization of that information [56]. Since knowledge and experience grow with age, children at the formal operational stage tend to perform better in most recall memory tasks than children in the concrete operational stage of development.

Social Aspects: Younger children's problem-solving approaches are influenced by what they observe or what they have been taught by adults and older children [57]. Therefore, family members and teachers play an important role in developing children's problem solving skills. Starting at the formal operational stage, however, adult influence decreases as children develop stronger ties with their peers [27].

2.3 Implications of Developmental Stages for Children's Privacy and Security Education

Assessing online risks often involves cognitively complex processing that younger children are not developmentally equipped to handle [117]. For example, Piaget's theory [132] suggests that children in the pre-operational stage (ages 2-7) have trouble identifying the credibility of online information [117], because they cannot see things from perspectives other than their own and recognize that others (e.g., advertisers) might have ulterior motives. Furthermore, children at this stage in their cognitive development are unlikely to self assess and correct their ways of thinking to make future decisions. This makes it difficult for children to transfer the lessons in educational programs to another situation [117]. Children in the concrete operational stage (ages 7-11) have greater ability than pre-occupational children to organize thoughts. Their logical reasoning is further developed and they have some problem-solving abilities. However, early concrete operational children still have some difficulties transferring logical principles from situation to situation [117]. The developmental challenges of younger children suggest that educational materials that teach children how to assess online information are better suited for children in the later concrete operational stage and formal operational stage of cognitive development, with the formal operational stage (11-16) being the most cognitively developed to make logical assessments of online information [117].

Interestingly though, however, children are increasingly exposed to technology and online activities at a young age. Research reports that children as young as 2 years old have accessed a mobile device [143]. Steeves [166] similarity reports that cell phones and smartphones are the primary devices used by Canadian children to go online. Close to half of nine-year-olds regularly have access to their own or someone else's phone. By age 13, more than half own a personal cell phone. The average time children spend on mobile devices rose from 45 minutes a day in 2011 to 1 hour and seven minutes per day in 2013 [143]. Common primary online activities of 7 to 13-year-olds are playing online games, and streaming TV shows or movies [143, 166]. This frequent online connectivity increases children's exposure to online privacy risks, where younger children are particularly vulnerable because they do not have the maturity, experience, or the knowledge to safely navigate online spaces.

There appears to be an increasing need to introduce children to privacy and security information at an earlier age than the formal operational stage, but Piaget's theory suggests that pre-occupational children are cognitively inapt to process cognitively complex information like privacy and security. Therefore, children in the concrete operational stage appear to provide the best opportunities for future children's privacy and security education research.

2.4 Sociological Views on Children's Safety

Children's perceptions of privacy and security are less developed than those of adults. As a result, they often need to be protected from online threats [150, 157], particularly because of their naïve perception of online content and communication [116]. The Children's Online Privacy Protection Act (COPPA) in the U.S. [55] highlights that parents are seen as carrying the primary responsibility for supervising their children's Internet use. Parents feel a responsibility to protect their children from external harm, and from themselves due to their lack of maturity, experience, and the capacity for judgment required to make online decisions. Furthermore, the public's perception that parents are bad parents if they do not know where their children are and what they are doing at all times puts social pressure on parents [183]. As a result, children are frequently put under adult scrutiny to keep them “safe” from potential harm [101]. This includes preventing children's exposure to violent and sexual content, “strangers”, offensive speech, and commercial messages [103]. Even though parents are often recommended to monitor children, research [103] suggests that monitoring is an ineffective method for protecting children online because parents could not reliably infer children's beliefs or intentions based on the information exchanges that children engage in without an understanding the social context. Furthermore, monitoring children could damage trust in parent-child relationships, and could be ethically inappropriate [103]. To what extent that children should be protected depends on the capacities for autonomy and reciprocal relationships of the particular child and his or her family [103]. Researchers suggest that more productive approaches include teaching children critical-thinking skills to facilitate their engagement with the online world [14], engaging children and parents in social co-use of technology, and using interactive mediation to involve families in ongoing conversations about online issues [103].

Chapter 3

Behaviour Model of Privacy and Security

Traditionally, computer security and privacy research has focused on technological countermeasures to protect end-users. Research now recognizes that technical improvements alone cannot adequately provide protection due to two reasons: First, privacy and security are moving targets where threats constantly change and evolve. Attackers actively work to evade or bypass protection mechanisms. For example, attackers create variations of malware to evade intrusion detection systems. Second, privacy and security mechanisms, at times, require non-expert users to make decisions. For example, users are responsible for adjusting their privacy settings, choosing strong passwords, and complying with security policies. Some experts argue that users should be kept out of the security decision loop [124], but due to the complexity and rapid evolution of threats, it is most likely that secure solutions in the near future will continue to include human interaction and decision-making. Unfortunately, attackers often exploit the human link in the security chain [1].

Research in security and privacy suggests that users engage in risky behaviour due to the following reasons. First, they have low motivation because privacy and security are secondary tasks and target behaviours are difficult to perform [182]. For example, authentication is necessary to prevent unauthorized access to user accounts, but people's primary task is to use their accounts, not to create and recall complex passwords. Furthermore, tasks in managing privacy and security could be difficult, time-consuming, and burdensome [182]. This ultimately reduces users' motivation [1]. Second, users have poor understanding of how privacy and security protection mechanisms work because of incomplete mental models [178]. Mental models are users' internal understanding of a system or process. These are not necessarily accurate or informed, but are applied by users for reasoning, learning of new concepts, and problem solving [39]. Unfortunately, users typically rely on poor mental models with

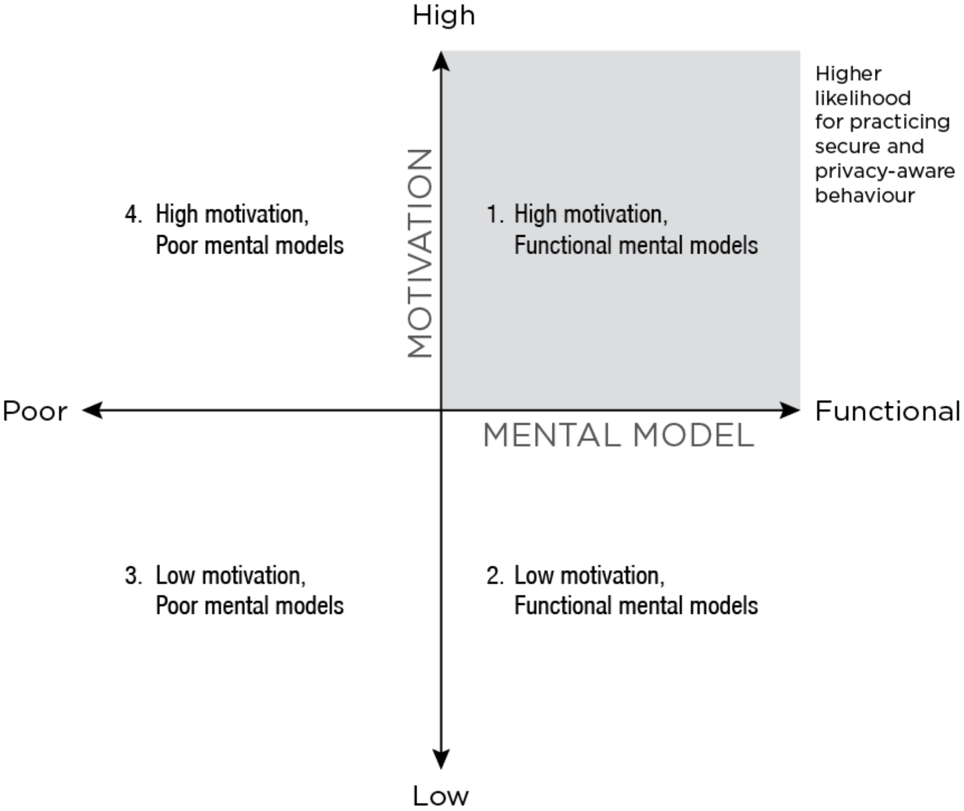

High
Higher likelihood for practicing secure and privacy-aware behaviour
MOTIVATION
4. High motivation, Poor mental models
1. High motivation, Functional mental models
Poor
Functional
MENTAL MODEL
3. Low motivation, Poor mental models
2. Low motivation, Functional mental models
Low

Figure 3.1: The Behaviour Model of Privacy and Security has two dimensions: motivation and mental models; and four behavioural states: 1) high motivation and functional mental models; 2) low motivation and functional mental models; 3) low motivation and poor mental models; 4) high motivation and poor mental models.

regards to technology and computer security, and this leads to erroneous decision-making [178].

Supported by these views, we propose a conceptual behaviour model that asserts the need for high motivation and functional mental models for users to achieve positive privacy and security behaviour change. We theorize how users' motivation and mental models affect privacy and security behaviour outcomes, and discuss the differences between privacy and security concerns.

3.1 Proposed Behaviour Model of Privacy and Security

Our proposed Behaviour Model of Privacy and Security (BMOPS) has two main dimensions, motivation and mental models. The model asserts that to achieve positive security behaviour outcomes, users need high motivation and functional mental models. Figure 3.1 visualizes the behaviour model's four behavioural states. The x-axis conceptually plots users' mental model state from *poor* to *functional.* The y-axis plots users' motivational state from *low* to *high.* As a conceptual model, the axes contain no units. Each quadrant demonstrates a behavioural state that influences the privacy and security behaviour outcome. Positive behaviour is unlikely to occur if users have low motivation and a poor mental model, low motivation and a functional mental model, or high motivation and a poor mental model.

3.2 Mental Models

Work in usable privacy and security [6, 71, 87, 178, 179] highlights that an important aspect of privacy and security management is users' existing knowledge about these issues and the technology they use. Users make decisions based on their existing mental models [178]. We know little of children's privacy and security mental models. We assume, however, that most factors affecting adults' mental models are also relevant to children, and that children's understanding of privacy and security concepts are less sophisticated than those of adult users.

Folk Models: Folk models represent aspects of mental models that are not necessarily correct in the real world, but are shared among members of a similar culture and are used for decision making [40]. Wash [178] identified eight folk models that are used for erroneous security decision-making. The folk models consisted of users' conceptualizations of "hackers": they are digital *graffiti* artists that cause mischief; they are *burglars* who break into computer systems; and they are *contractors* who support organized crime. Some thought hackers only target *big fish*, while ordinary people are unlikely victims. Four other folk models included models of "viruses": they are generally *bad*; they are *buggy software*, they cause *mischief*; and they *support crime.*

Hogan [82] suggests that users perceive presentation of self such as status updates and photo-sharing in online social spaces as *public exhibitions* instead of *personal performances.* They view themselves as *curators* that manage and redistribute this digital content in their personal exhibition spaces. Burkell et al. [21] suggest, however, that these perceptions apply largely to information posted by *others.* Users frame their own online participation based on their own orientation towards privacy. Users view their online profiles as *spaces for social display with a controlled audience*, *spaces for social display with an open audience*, or as *places to post personal information to a controlled audience* [21].

Rader et al. [134] suggest that folk models come from learning privacy and security information informally from other people. Non-expert computer users tend to retell online incidents that they have experienced in a way that is not particularly accurate or sophisticated [178], but can nevertheless impact the way other people think about privacy and security, and their subsequent behaviour during decision-making.

Expert vs. Novice Models: When novice computer users receive online advice from "experts", disparities often exist in the communicated risk and the recipients' perceptions of the risk, which could lead to ineffective risk communication [6]. This is because computer security experts have different mental models than novice users [6]. Expert mental models are more technically correct than folk models, but they may be ineffective for communicating computer security concepts to novice users.

For privacy, inconsistencies exist between public expectations and social norms [22]. For example, even though service providers of social media claim they are private spaces, users of social media view and treat online social networks as public venues [22].

Several researchers (e.g., [6, 178]) advocate that the effectiveness of privacy and security communication could increase if it was adjusted to work with users' current mental models, and that users do not necessarily have to learn about intricate technical details to achieve desirable behaviour.

Risk Communication: Effective end-user risk communication relies on how well the conceptual models embedded in the message match end-users' perceptions of the risk [6]. Camp [87] identified five privacy and security conceptual models: *physical privacy and security*, *medical infections*, *criminal behaviour*, *warfare*, and *economic failure*. Within these models, dread characteristics such as rare and catastrophic events were found to be the biggest driver of risk perception, where greater dread is correlated with greater severity of the perceived risk [65]. This suggests that perceived severity have a major influence on users' behaviour.

Metaphors: Conceptual models of computer privacy and security rely heavily on the use of metaphors to communicate complex concepts to the general population [87]. Physical privacy and security metaphors use physical objects like locks and keys to signify individualized and localized control, and eyes and security cameras to signify monitoring and surveillance. The medical infection model of security is grounded in the infectious diseases epidemic metaphor. The criminal behaviour model depicts privacy and security breaches as metaphors of crime where users and machines are victims. The warfare concept implies the existence of a determined implacable enemy. Lastly, vulnerabilities are perceived as economic failures, such as security failures causing downtime and costs. In our earlier studies that use metaphors in infographics to teach user about passwords [187], malware [188], and privacy [114], we found that using metaphors to teach users about privacy and security concepts was perceived to be more effective and showed greater increase in knowledge than text-only information. Metaphors are most useful to help users fill in the details from their experiences with familiar concepts, but may not support a complete mental model of the target domain [100].

3.3 Security Motivation

Traditionally, information security research has identified low motivation and insecure work practices as the main causes of security problems [60]. This attitude assumes that users are inherently not motivated to adopt safe behaviours. Users are viewed as hopelessly lazy and doing the minimum possible. On the contrary, usable security researchers have found that insecure practices and low motivation can be caused by many other factors such as usability issues [1, 30, 182], poor mental models [6, 178], and misconceptions of the risks.

Susceptibility: Users make security decisions based on their self-assessed susceptibility to a threat, the severity of threat, and the likelihood that they will be affected [146]. Many users hold the belief that they are unlikely targets for cyber criminals because hackers have little to gain from people who are neither rich nor famous [178]. With this mindset, protecting against cyber-crimes is not a high priority.

Cost/Benefit Tradeoff: Users often analyze the cost and benefit of security advice to make rationalized judgments about whether following the advice is worth their time, cost, and effort. Herley [80] argues that the cost-benefit tradeoff for most security advice is unfavourable; its intention is to shield users against direct cost of attacks, but burdens users with indirect costs in the form of continuous preventative effort. Furthermore, cost-benefit judgment calls can often be flawed because people do not have the knowledge to fully assess the magnitude and likelihood of the harm [172].

Self-Efficacy: Users make calculated decisions based on the perceived efficacy of the threat response and their own capabilities in completing tasks required for the desired response [96, 155]. Rhee et al. [141] found that greater feelings of self-efficacy is correlated to secure behaviours. However, secure behaviours motivated by self-efficacy may change depending on other variables, such as self-assessment of the user's susceptibility [146] and the availability of resources [79].

Perceived benefits: Users' personal perceived ease of use and perceived usefulness of a security system are correlated to users' intention to act securely [158]. Improving the usability of security systems, however, may not be enough to induce behaviour change. Prior work in security software adoption studies (e.g., [177], [184]) suggests that traditional theories of technology acceptance (e.g., Technology Acceptance Model [41], Protection Motivation Theory [146]) do not fully reflect users' motivation to adopt security software. This is because the management of security systems is a secondary task [182]. Users, therefore, do not perceived security tasks as supporting their work activities directly.

Fear: Fear is often used as a means to enforce compliance and control [24]. Fear is a powerful motivator, but not necessarily ethical or empowering [59]. Furthermore, fear as a motivator can have unintended effects in computer security. Researchers [59] found that behavioural outcomes from fear can be unpredictable because of variations in users' perception of the threats and how susceptible they are to the threat.

Personal Responsibility: An estimated 90% of home computer users feel responsible for securing their personal computers [62]. This greatly exceeds prior assumptions about users' personal motivation. LaRose et al. [96] found that users who believe online safety is their personal responsibility are significantly more likely to protect themselves. In some cases, users have sufficient motivation to practice computer security, but other factors influence their ability to achieve the desired security outcome.

As discussed earlier, security decisions are often made based on poor mental models that lead to incorrect assessment of the risks and protective response. Poor security behaviour can therefore ensue even though users feel responsible for protecting their computers.

Social Responsibility: The desire to act in a socially responsible manner may influence users' cost-benefit tradeoff analysis even though the benefit may not be for the users themselves [3]. Although at times, socially induced behaviours could be motivated by self-interested reasons like social acceptance and social rejection [59]. Users may feel a responsibility to warn others about security incidences that they have experienced. Rader et al. [134] found that most people do indeed learn security lessons from family and friends, and this impacts the way they think about security and their subsequent behaviour when making security-relevant decisions.

3.4 Privacy Motivation

Privacy behaviour is more likely to be personally and socially motivated than security, and includes individuals' ability and right to exert control over how information flows, who has access to it, and in what context [173].

Social Need: Sharing parts of ourselves is a social need. People choose to disclose information about themselves because they strive to make personal connections [173]. At the same time, people are also concerned about what other people know about them, what information they share with whom, where, and in what context [173]. Research suggest that even though young people share a lot of personal information with peers, they are just as concerned about their privacy as adults, but lack the skills or resources to manage their privacy as effectively as adults [83].

Sense of Control: Users' sense of control over content and audience in social media leads to different privacy needs and expectations [21]. Presentation of self in online social spaces such as status updates and photo-sharing are seen by users as public exhibitions instead of personal performances; participants view themselves as curators that manage and redistribute content in their personal exhibition spaces [82]. Burkell et al. [21] suggest that users have different orientations towards privacy. Those who view online profiles as open spaces exercise little control over content or audience, while those who view online profiles as social spaces or as places to post personal information to a selective audience exercise more control over content and audience.

Context: Notions of privacy are context-dependent where users share information for particular purposes in particular contexts. Nissenbaum [126] argues that the "contextual integrity" of privacy is violated when information is used for other purposes or context than it was originally shared. The concept of contextual integrity is particularity relevant in understanding privacy preferences between different user groups; for example, children and adults often have different social contexts in which they disclose information and thus have different privacy needs.

Nothing to Hide: The misconception that no problem exists if a person has nothing to hide permeates the popular discourse about privacy issues relating to government and data surveillance [164]. People with the "I've got nothing to hide, therefore I have nothing to fear" attitude towards privacy believes that no threats to privacy exists if an individual has nothing sensitive, embarrassing, or illegal to conceal. Solove [164] argues that privacy viewed from this perspective, as a form of concealment or secrecy. It ignores the fact that privacy is also about control, context, and willing disclosure.

Trust: Sharing of private information is often used between people to demonstrate trust and intimacy. A study [159] found that couples often share banking information to manage money. Pew Internet research [97] found that 30% of teens surveyed give a friend, boyfriend, or girlfriend access to their personal accounts as a demonstration of trust and intimacy. However, there is also evidence that password sharing is based on nuanced and careful decisions people make about what passwords to share and with whom [89].

3.5 Privacy vs. Security

Privacy and security threats are often seen as synonymous. However, user-centered theories of privacy [10] view it as a separate and distinct consideration from security. For example, Bambauer [10] defines privacy as "a normative framework for deciding who should legitimately have the capability to access and alter information." Security, in contrast to privacy, "is the set of technological mechanisms that mediates requests for access or control."

Security assumes a threat model and assesses precautions against a determined attacker. For example, password guessing attacks could be mitigated by analyzing the system's vulnerabilities to the types of attack (e.g., brute-force and dictionary), and devising countermeasures to mitigate the threats to the system against a malicious attacker whose intention is to gain unauthorized access, or make unauthorized use of the protected data. Security demands "correct" behaviour from users that are usually defined by a set of rules of what should or should not be done (e.g., create strong passwords; do not reuse passwords). Furthermore, it assumes that more security is better than less security, and that "secure" behaviour from users is always desirable.

Privacy threat models are less holistic than security because attackers are more likely to be socially motivated. For example, attackers could be a vengeful ex or a former friend sabotaging the user's account, spreading humiliating messages, or scouring private messages for clues of disloyalty or infidelity [142]. Privacy concepts are also personal, and differ across individuals. The Westin Index [181], a privacy index created from a series of privacy surveys, categorized people's privacy concerns into three types: fundamentalist, pragmatic, and unconcerned. According to the research, approximately 25% of consumers are fundamentals that have a strong distrust of organizations collecting personal information, and would choose more privacy over service benefits. On the opposite spectrum are the unconcerned who are more trustful and comfortable giving personal information in exchange for secure service benefits. They account for approximately 18% of consumers. More than half (57%) of consumers are pragmatists, who weigh the tradeoffs between various consumer benefits and degrees of intrusiveness of personal information. For many users, therefore, privacy decisions are based on a series of tradeoffs that each person weighs for themselves in different contexts. There may be certain situations when more privacy is undesirable, such as when people try to make personal connections and strive to be socially active. The immediate benefits and gratification that people receive from sharing parts of themselves might outweigh the potential long-term consequences of disclosure. Therefore, there is no clear "correct" behaviour for everyone. Individuals make decisions appropriate to their circumstances, attitudes, and goals.

However, a common property between privacy and security is that the damage caused by breaches cannot be undone. Even if a system is left unsecured for a short period of time, it cannot be ascertained that it has not been compromised. Similarly, once private information is disclosed, it cannot be undisclosed. Therefore, it is important for users to understand the potential consequences of their actions, so they can make informed privacy and security decisions.

Our behaviour model provides a general conceptual framework for understanding two major factors, mental models and motivation, for influencing user behaviour. It assumes that privacy and security decisions are made based on individual choices guided by the users' mental models and motivations behind the choice. The model does not address, however, the complexity of user motivation and tradeoffs relating to privacy and security, or users' individual differences. We acknowledge that users may have different motivations for privacy and security concerns that should be taken into consideration. Nevertheless, users need functional mental models to understand the potential consequences of their actions, so they can be in an informed position to assess the tradeoffs. The conceptual model provides a way to think about the relationship between mental models and motivation in explaining user behaviour.

Chapter 4

Design Principles for Privacy and Security Education

In this chapter, we introduce a set of established design principles from persuasive technology and instructional design, then review and analyze existing privacy and security education work for adults and children to identify which principles were used. We discuss the differences in design between children and adults' privacy and security educational systems, and identify the research gaps. We end the chapter with a research roadmap that describes our rationale for the work presented in the subsequent chapters. Partial work presented in Sections 4.1 and 4.2 of this chapter was published in the International Journal of Human-Computer Interaction in 2016 [189].

4.1 Revisiting Design Principles for Adults

Researchers in education and persuasive technology have developed a set of persuasive technology principles (PT) [58] and instructional design principles (ID) [63]. PT principles (summarized in Table 4.1) guide the design of interactive computing systems intended to change people's attitudes and behaviour [58]. ID principles (summarized in Table 4.2) guide the design of effective and appealing instructional materials [63]. Although these design principles were not initially developed for children, they are generic enough to be applicable to children, and are highly relevant to the design of children's educational materials.

The set of PT and ID design principles are selected because they help to address two main challenges in privacy and security education.

Challenge 1: Privacy and Security are a Secondary Concern. Users are uninterested in privacy and security because they are secondary tasks [182] in their everyday computer interactions. Children's primary tasks on mobile devices include playing games, watching video clips, messaging, posting images, and doing school work [99, 143, 166]. Like adults, they typically do not regard managing their privacy

		Persuasive Technology Principles	
MO	MM	**Principle**	**Description**
●	◐	*Reduction*	Reduce complex behaviour into simple tasks to help users perform the target behaviour.
●	◐	*Tunnelling*	Guide users through a process to provide opportunities to persuade along the way.
●	◐	*Personalization*	Personalize content to achieve a greater capability for persuasion.
●		*Conditioning*	Positively reinforce a behaviour by giving users praise and rewards.
●	◐	*Suggestion*	Offer users fitting suggestions to have greater persuasive powers.
●	●	*Tailoring*	Tailor information to factors (needs, interests, age, usage context) relevant to the user group.
●		*Social Cues*	Provide social cues from the system to persuade users by social influence.
	●	*Simulation*	Enable users to observe cause and effect relationships though simulations.
◐	◐	*Monitoring*	Track users' performance or status to make behavioural patterns more transparent.
●	●	*Rehearsal*	Rehearse a behaviour within a system to reinforce a similar behaviour in the real world.
●	●	*Procedural Rhetoric*	Allow users to explore rule-based representations and interactions to persuade users toward a certain position.

Table 4.1: Design principles for persuasive technology [58]. MO = motivation, MM = mental models, ● = strongly supports the property; ◐ = weakly supports the property; *no circle* = does not support the property.

		Instructional Design Principles	
MO	MM	**Principle**	**Description**
◐	●	*Segmenting*	Segment information into learner-paced chunks to give users opportunities to pause, process, and reflect before continuing to the next step.
	●	*Contiguity*	Present words and corresponding images contiguously to increase learning performance.
●	●	*Reflection*	Provide users with opportunities to reflect on what they learned to increase learning.
●	●	*Feedback*	Provide immediate feedback helps users to assess how they are doing.
●	●	*Narrative*	Present training material within the context of a story to enhance learning.
◐	●	*Signalling*	Direct user attention to key messages in the lesson to help with information discovery and understanding.
●		*Socialization*	Attribute social characteristics to the user interface that resemble human-to-human interaction help to engage users.
	●	*Multimedia*	Use words and graphics to increase learning rather than just text or graphics alone.
●	●	*Conceptual&Procedural*	Show causual relationships between conceptual knowledge (e.g., mental representation of an idea) and procedural knowledge (e.g., steps to solve a problem or complete a task).

Table 4.2: Design principles for instructional design [63]. MO = motivation, MM = mental models, ● = strongly supports the property; ◐ = weakly supports the property; *no circle* = does not support the property.

and security as a primary concern and may be even less likely to understand the possible consequences of their insecure actions. Therefore, methods of capturing the users' interest and helping them to stay on task are necessary in the design of privacy and security educational tools. For example, PT principles like *tailoring* and *conditioning*, and ID principles like *multimedia*, *socialization* and *narrative* could be used to activate learning and create engagement to address this problem. In addition to increasing users' motivation to learn about privacy and security, it is also necessary to persuade users toward practicing privacy-conscious and secure behaviour. PT principles like *suggestion*, *social cues*, *rehearsal*, and *procedural rhetoric* could be applied in educational tools to persuade and shape behaviour.

Challenge 2: Privacy and Security Concepts are Difficult to Understand. Privacy and security systems are often too complex and abstract for end-users to form proper mental models and use accurately [31]. Usability studies of modern security software such as password managers found that these software have poor usability and that many users have difficulties using them effectively [31]. Even though children rarely manage advanced privacy and security mechanisms, they encounter situations through online interaction that requires them to make decisions relating to disclosing personal information, entering passwords, downloading apps, and posting online content [166]. These decisions could have potential consequences for the child and others, such as friends and family.

Work in usable privacy security found that improvement in user knowledge and awareness could motivate them toward secure practices, because motivation to comply is based on the understanding why their behaviour can put themselves or others at risk [1]. The applications of PT and ID principles could make privacy and security information more accessible and understandable for children, which could ultimately affect their online behaviour. For example, PT principles like *reduction* and ID principles like *segmenting* and *signalling* could make security lessons easier to absorb. Further, ID principles of *contiguity*, *conceptual and procedural knowledge*, *reflection*, and *immediate feedback* could help users to build good mental models so they can make secure and privacy-conscious decisions.

To assess the effectiveness of the principles on how well they support motivation and mental models from our Behaviour Model introduced in Chapter 3, we conducted an analysis of the principles. In Tables 4.1 and 4.2, the principles are shown to either strongly support, weakly support, or do not support privacy and security motivation and mental models when applied to the design of education materials. In general, many principles for persuasive technology design strongly support the property of *motivation*, but weakly support the property of *mental models*. For example, the PT principle of *conditioning* (i.e., giving users praise and rewards to reinforce a behaviour) strongly supports users' motivation, but it does not help them make informed decisions by developing functional mental models. Some principles, like *reduction* (i.e., simplifying complex behaviour), strongly support users' motivation because they make the task easier to do, but may leave gaps in users' mental models, and therefore, weakly support them.

In comparison, principles for instructional design are divided in their strengths for supporting motivation and mental models. For example, the ID principles of *multimedia*, *contiguity*, *signalling*, and *segmenting* reduce the cognitive load, enhance comprehension, and increase long-term memory [34, 106], but they do not necessarily increase users' motivation to practice privacy and security.

We also found some parallels between persuasive principles and instructional design that mutually reinforce one another. The aforementioned ID principles may help to reinforce the PT principle of *reduction*, which states that by making a behaviour easy to do, users are more likely to complete the task [58]. If privacy and security information is easy to learn, understand, and persuasive in its message, it would be more likely to lead to message absorption and changes in attitude or behaviour. Other pairs of principles like *social cues* (PT) and *socialization* (ID), *conditioning* (PT) and *feedback* (ID), or *reduction* (PT) and *segmenting* (ID), have related design functions that may be used in conjunction to increase their effectiveness.

4.2 Applying Design Principles to Privacy and Security Education

We reviewed existing privacy and security education materials and identified which PT and ID principles were utilized. The result is summarized in Table 4.7. A work is shown to employ the principle if used explicitly in the system, even if it is not originally identified by its authors. We found more educational efforts toward adult users than toward children. In Tables 4.3, 4.4, and 4.5, we reviewed privacy and security education work created for adults, and in Table 4.6, we reviewed educational work created for children. First, the tables list the names of the systems. Second, we identified the systems' media type: These include computer/online games, comics, physical tabletop games, visualizations, learning modules of linearly presented educational content, and "just-in-time" systems that provide educational information when a user has taken insecure actions. Third, we classified the target audience intended by the original authors and creators. Fourth, the privacy and security topics that were addressed by the systems are listed. The fifth column identifies whether the systems have been empirically tested with users in experiments or user studies. Lastly, we give brief summaries of the systems and how they work.

For organizational purposes, we discuss the literature in detail by media type. The categories are: educational games (Section 4.2.1), comics (Section 4.2.2), tabletop games (Section 4.2.3), visualizations (Section 4.2.4), learning modules (Section 4.2.5), and "just-in-time" systems (Section 4.2.6). Many design principles can be used effectively across different media. For example, the principle of *procedural rhetoric* was developed in computer game theory [15], but could be applied to other interactive systems, as shown in our analysis of existing education work in Table 4.7. To prevent overlap and repetitiveness in the following sections, we focus on discussing the design principles that are most commonly represented by the media type, and give examples of how they are used in existing work.

4.2.1 Educational Games

An important source of motivation for learning is interest in the activity [175]. Children's play is inherently associated with learning [147]. Educational games fuse entertainment aspects of gameplay with learning. Games are a promising education tool because gameplay in intrinsically motivating [144]; the game environment enables exploration, problem solving, and incidental learning. However, a challenge in educational games is balancing fun aspects of gameplay with educational goals [144]. Several persuasive principles are highly applicable to educational game design.

Name	Type	Target Users	Topic(s)	Empirical	Description
A. Anti-Phishing Phil [156]	Computer Game	End-users	Phishing	Yes	The fishing game teaches users how to use cues in URLs to avoid falling for phishing. Users play as the fish character Phil who must avoid eating lures of fake worms (i.e., phishing links).
B. Auction Hero [29]	Computer Game	End-users	Phishing, Malware	Preliminary	Auction Hero models real life by making security a secondary consideration while the primary game activity is making profitable transactions buying and selling robot parts online.
C. CyberCIEGE [38]	Computer Game	Corporate users	Network Security	Preliminary	The simulation game enables players to construct, configure, operate, and defend their computer networks against hackers, and watch the consequences of their choices.
D. Secure Comics [189]	Comic	End-users	Passwords, Malware, Privacy	Yes	The interactive comic book teaches various risks and protection strategies while telling the story of cyber-detectives Jack and Nina solving computer security crimes to protect the public from the cyber-villain Hack.
E. Security Cartoons [165]	Comic	End-users	Phishing, Malware	No	Short comic strips are designed to improve non-expert users' understanding of Internet security.
F. Privacy Notice Comics [91]	Comic	End-users	Privacy Notices	Proposed	Comics were proposed as a medium to make privacy and security notices more accessible and comprehensible, especially for low literacy Internet users.

Table 4.3: Adult privacy and security education, part I.

Name	Type	Target Users	Topic(s)	Empirical	Description
G. Security Infographics [114,187,188]	Visualization	End-users	Passwords, Malware, Privacy	Yes	Conventional security metaphors (e.g., a lock as a metaphor for a password) are used in infographics to improve security risk communication and understanding.
H. Anti-Phishing Program [5]	Visualization	End-users	Phishing	No	The program re-purposes inactive phishing URLs to re-direct users to an educational page when they have clicked on a phishing link. The landing page teaches users about phishing and gives step-by-step advice for phishing prevention.
I. Privacy Nutrition Label [90]	Visualization	End-users	Privacy policies	Yes	The privacy label uses design elements and principles from nutrition, warnings, energy labelling, and banking notifications to make privacy policies quicker to read and easier understand than existing natural language privacy policies.
J. Firewall Metaphors [135]	Visualization	End-users	Firewall warnings	Yes	The personal firewall design uses physical security metaphors (brick wall, locked door, bandit) to improve comprehension, enhance risk communication, and increase the likelihood of safe behaviour compared to warning messages from existing firewall software.
K. Geo-Phisher [190]	Visualization	End-users	Phishing	Yes	The interactive information visualization tool uses a scatterplot map to plot the temporal and geographical information of blacklisted phishing URLs to provide context for phishing crimes.

Table 4.4: Adult privacy and security education, part II.

Name	Type	Target Users	Topic(s)	Empirical	Description
L. Ctrl-Alt-Hack [45]	Card Game	CS/STEM Students	General Computer Security	No	Security concepts are embedded into a hacker-themed strategy card game to increase security awareness and understanding.
M. Privacy Game [12]	Card Game	End-users	Privacy	No	The card game enables players to take on a variety of roles to make decisions regarding the collection and arrangement of personal data, making some public and keeping other types private.
N. Smells Phishy? [13]	Board Game	End-users	Privacy	Yes	The tabletop board game educates users about online phishing scams and how to avoid them while making purchasing decisions shopping at several e-commerce stores.
O. [d0x3d!] [69]	Board Game	CS/STEM Students	Network Security	Preliminary	The collaborative tabletop game enables players to win or lose as a group by taking on the role of white-hat hackers to learn about network security.
P. PhishGuru [94]	Email System	Corporate Users	Phishing	Yes	The email-based anti-phishing education explains phishing risks and prevention tips after users have fallen for a simulated phishing attack through their email.
Q. Privacy Leaks [9]	Mobile App	End-users	Privacy	Yes	The app enables users to self-monitor the frequency and destination of users' shared data. Feedback is given as just-in-time notifications to alert users the moment the data is being sent.

Table 4.5: Adult privacy and security education, part III.

Name	Type	Target Age	Topic(s)	Empirical	Description
A. Social Smarts [170]	Graphic Novel	Tweens and younger teens	Privacy	No	The graphic novel tells the story of two siblings who encounter privacy risks related to social networking, mobile devices, and gaming.
B. Co-Co's AdverSmarts [110]	Learning Module	Ages 5–8	Targeted Marketing	No	Players help the character Co-Co Crunch create a commercial website through selecting special features and learn about marketing techniques that target children in the process.
C. Privacy Pirates [111]	Learning Module	Ages 7–9	Privacy	No	The quiz module challenges the player to answer private and personal questions on the Internet and rewards correct choices with map pieces that leads to the pirate's treasure.
D. Privacy Playground [112]	Learning Module	Ages 8–10	Marketing, predators, bullying	No	The animated module follows the story of the CyberPigs as they encounter marketing ploys, spam, cyberbullying, and online predators.
E. Click if You Agree [109]	Learning Module	Ages 12–14	Privacy policies	No	The module teaches children how to identify the most important parts of privacy policies.
F. A Day in the Life of the Jos [113]	Online Game	Ages 11–14	Privacy	Yes	Players make privacy decisions for characters Jo and Josie that have consequences on their social media feed in this scenario-based game.
G. Smokescreen [161]	Online Game	Ages 14–16	Social Networking	No	The immersive game enables players to explore websites, search for clues, receive phone calls, chat on IM, and play minigames to simulate life online to teach about social networking risks.
H. The Watchers [137]	Hybrid Board/Computer Game	Ages 11–12	Privacy	Yes	The board game is augmented with computer-game elements that give players feedback about the consequences of their private information sharing decisions with individuals or companies.

Table 4.6: Child privacy and security education

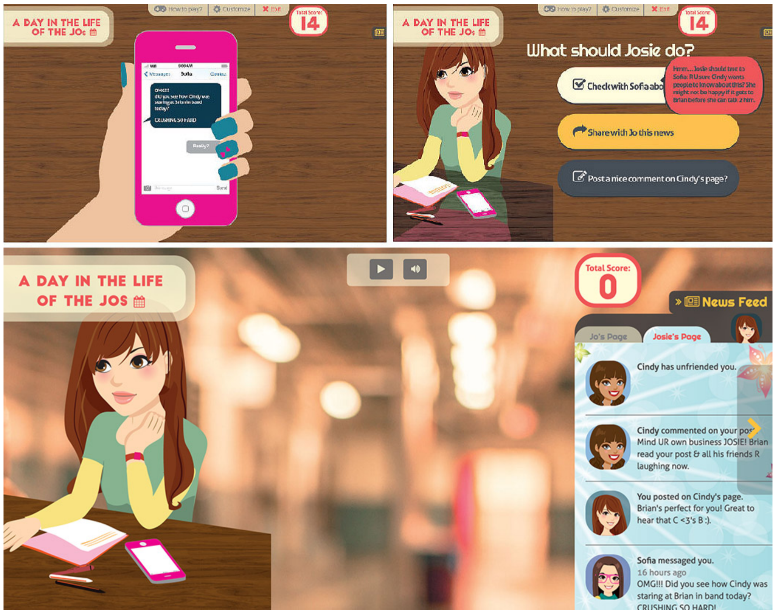
PT & ID Principles	A. Anti-Phishing Phil	B. Auction Hero	C. CyberCIEGE	D. Secure Comics	E. Security Cartoons	F. Privacy Notices Comics	G. Security Infographics	H. Anti-Phishing Program	I. Privacy Nutrition Label	J. Firewall Metaphors	K. GeoPhisher	L. Ctrl-Alt-Hack	M. Privacy Game	N. Smells Phishy?	O. [d0x3d!]	P. PhishGuru	Q. Privacy Leaks	A. Social Smarts	B. Co-Co's AdverSmarts	C. Privacy Pirates	D. Privacy Playground	E. Click if You Agree	F. Life of the Jos	G. Smokescreen	H. The Watchers
Reduction	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
Tunneling				♦	♦			♦	♦			♦				♦		♦	♦	♦	♦	♦	♦		
Personalization			♦														♦								
Conditioning	♦	♦		♦							♦								♦	♦	♦		♦		
Suggestion	♦	♦		♦		♦		♦		♦	♦			♦					♦	♦	♦	♦	♦		♦
Tailoring	♦	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦
Social Cues	♦	♦	♦	♦	♦								♦	♦	♦	♦		♦	♦		♦		♦	♦	♦
Simulation	♦	♦	♦					♦			♦	♦	♦	♦	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦
Monitoring			♦					♦								♦	♦							♦	
Rehearsal	♦	♦	♦					♦				♦		♦	♦							♦	♦	♦	
Procedural Rhetoric	♦	♦	♦	♦								♦	♦	♦	♦	♦			♦		♦		♦	♦	♦
Segmenting	♦	♦	♦	♦	♦	♦					♦	♦	♦	♦	♦			♦	♦	♦	♦	♦	♦	♦	♦
Contiguity	♦			♦	♦	♦	♦	♦		♦						♦		♦					♦		
Reflection	♦	♦	♦	♦		♦		♦		♦	♦	♦	♦	♦	♦	♦	♦		♦		♦	♦	♦	♦	♦
Immediate Feedback	♦	♦		♦				♦			♦	♦		♦					♦	♦	♦	♦	♦		♦
Narrative	♦			♦	♦	♦						♦		♦				♦			♦		♦	♦	♦
Signalling	♦	♦		♦		♦	♦	♦	♦	♦						♦	♦		♦		♦	♦	♦		
Socialization	♦	♦	♦	♦	♦	♦	♦	♦				♦	♦	♦		♦		♦		♦	♦	♦	♦	♦	♦
Multimedia	♦	♦	♦	♦	♦					♦		♦				♦	♦		♦	♦	♦	♦	♦	♦	♦
Conceptual&Procedural	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦	♦	♦			♦			♦	♦	♦	♦

Table 4.7: Summary of PT and ID design principles used in privacy and security education for adults (left column) and children (right column). ♦ = work that uses the principle. ■ = Evaluated. Descriptions of adults' educational systems can be found by the corresponding letter code in Tables 4.3, 4.4, and 4.5; Descriptions of children's systems can be found in Table 4.6.

The Procedural Rhetoric Principle (PT): A powerful persuasive principle employed in computer games is procedural rhetoric. The concept was developed by Bogost [15] as part of his theoretical work on persuasive games, which are video games that aim to educate users through gameplay. Rhetorical appeal is discovered by users through interaction with the system. In CyberCIEGE [38], the game achieves procedural rhetoric through computer network management simulations, where players interact with the system to construct, configure, and protect computer networks necessary to allow virtual users to be productive and achieve goals to further the success of the enterprise. Through simulated procedures, players observe the consequences of their choices and gain awareness of organizational security needs and challenges. In a game called Smokescreen [161] created for teens, the game achieves procedural rhetoric through simulations of life on the Internet. Players use “Fakebook”, “Gaggle”, “Tweetr”, “MSG messenger” to interact with in-game characters. Teens are persuaded towards practicing safer actions on social media as they recognize the risks and threats contained in the fictional game could be real.

The Conditioning Principle (PT): Conditioning positively reinforces a target behaviour [58], such as giving praise and rewards. Conditioning provides users with immediate positive feedback and encourages users to continue playing. For example, users are rewarded with game money and reputation points for trading robot parts while staying vigilant against security risks in Auction Hero [29]. This helps users to stay motivated in the game and reinforces the positive security behaviours learned.

The Social Cues Principle (PT): Social Cues from computers has significant implications for persuasion because people respond socially to computers [58]. Computer games leverage social influence to motivate and persuade users to learn. Characters could be designed with anthropomorphism to give them humanistic and emotional appeal. As a pun for phishing, “Anti-phishing Phil” [156] is centred around a family of fish characters, with the father providing advice to his son Phil. Social presence could also be psychological. It is suggested that characters designed with a sense of humour are perceived to be well rounded, interesting, and more believable [125]. Research in serious games found that the use of humour eases the social, emotional, and cognitive challenges of serious topics, and enriches the overall user experience [49].



OMG!!!
did you see how Cindy was staring at Brian in band today?
CRUSHING SO HARD

Really?

Hmm... Josie should text to Sofia: R U sure Cindy wants people to know about this? She might not be happy if it gets to Brian before she can talk 2 him.

Cindy has unfriended you.

Cindy commented on your pos Mind UR own business JOSIE! Brian read your post & all his friends R laughing now.

You posted on Cindy's page. Brian's perfect for you! Great to hear that C <3's B :).

Sofia messaged you.
16 hours ago
OMG!!! Did you see how Cindy was staring at Brian in band today? CRUSHING SO HARD!

Figure 4.1: The cyberbullying segment of the simulation game, A Day in the Life of the Jos [113]. The character Josie receives a text message (top left), and the player decides what Josie should do from a list of options (top right). The consequence of the player's action is immediately displayed in Josie's social media feed (bottom).

The fact that people respond socially to computers has significant implications for persuasion. It opens the door for computers to apply a host of persuasive strategies that are collectively described as social influence that arises from social situations.

The Rehearsal Principle (PT): Rehearsing a target behaviour within a system could enable users to change their attitude or behaviour in the real world. Systems that simulate certain aspects of the user's real environment are best equipped to achieve this. For example, in the scenario-based game, A Day in the Life of the Jos [113], players must act within simulated situations that are relatable to the tweens' life. Figure 4.1 shows the cyberbullying segment of the game where the character Josie is faced with a decision and has to respond to a mean text message about a friend. The game gives tweens the opportunity to rehearse how to respond in an appropriate manner, which could help them navigate similar situations they encounter in real life.

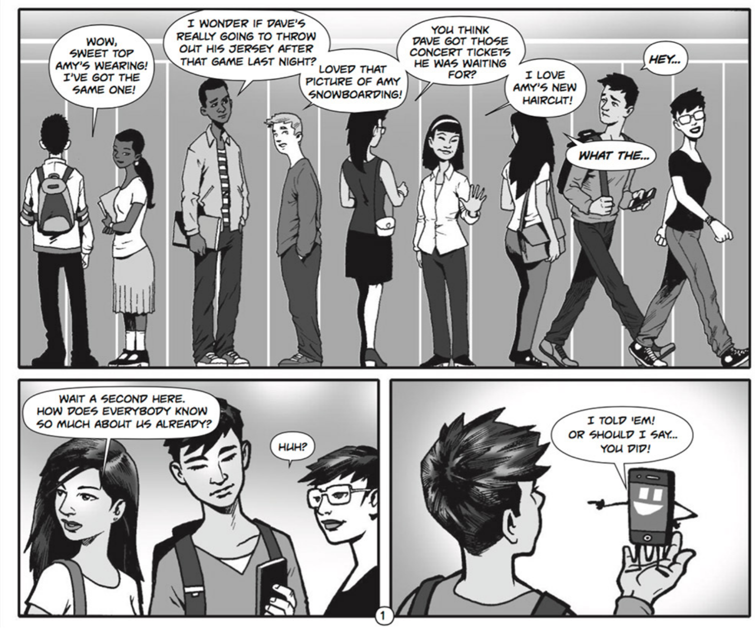

WOW, SWEET TOP AMY'S WEARING! I'VE GOT THE SAME ONE!
I WONDER IF DAVE'S REALLY GOING TO THROW OUT HIS JERSEY AFTER THAT GAME LAST NIGHT?
LOVED THAT PICTURE OF AMY SNOWBOARDING!
YOU THINK DAVE GOT THOSE CONCERT TICKETS HE WAS WAITING FOR?
I LOVE AMY'S NEW HAIRCUT!
HEY...
WHAT THE...
WAIT A SECOND HERE. HOW DOES EVERYBODY KNOW SO MUCH ABOUT US ALREADY?
HUH?
I TOLD 'EM! OR SHOULD I SAY... YOU DID!
1

Figure 4.2: A segment from the Social Smarts graphic novel [170].

4.2.2 Comics

Comics are motivating to read, visual, permanent (in contrast to "time-bound" media like film or animation), intermediary, and popular among children and youth [185]. Comics have fostered students' interest in science and aided in knowledge retention [123]. In security education, Srikwan and Jakobsson [165] proposed that online comic strips offer greater accessibility and immersion in the material than traditional security education efforts. Kumaraguru et al. [94] found that users who received comic strip interventions performed security-related tasks better than text/graphic interventions. Other studies on security comics found improved security understanding and motivated positive changes in security management behaviour [188, 189].

The Narrative Principle (ID): Learning is believed to be more effective if the training material is presented within the context of a story [104]. Several works have included narratives, but the most notable security narratives are told through comics. Comics that present stories about interrelated privacy consequences were proposed to simplify complex privacy notices [91]. Narratives could be segmented short stories in newspaper comic strip style like Security Cartoons [165], or be told through longer narratives like the Secure Comics comic book series [189]. Graphic novels usually wrap up the narrative in one or two parts like a book, as it is seen in Social Smarts [170], a short graphic novel created for tweens and teens that tells the story of a brother and sister as they navigate privacy risks to help young people navigate privacy issues in the online world with the help of their phone (see Figure 4.2).

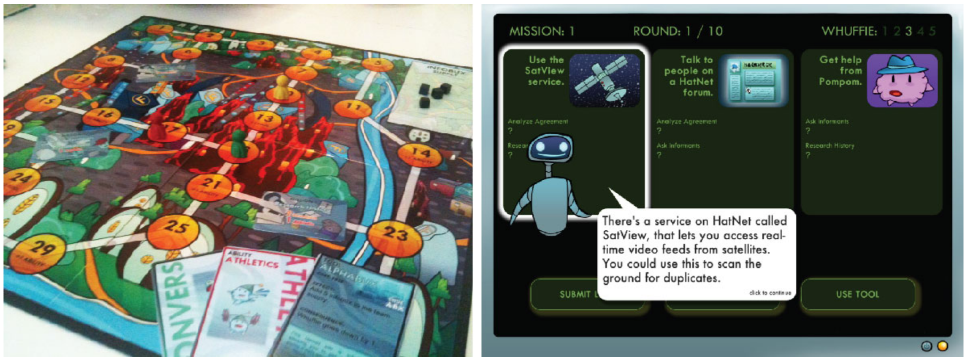
The Contiguity Principle (ID): When text is integrated on the screen close to related visuals, learning is more effective than when they are placed in isolation [106]. When visuals show relationships between elements being described in the text, they help to facilitate the construction of a mental model [75]. Text and images in comics are inherently contiguous. An eye-tracking experiment of Secure Comics [189] drew possible connections between visual attention and comprehension of the information. A user study of the comic found excellent information retention after one week and improved security knowledge and behaviour [189].

The Segmenting Principle (ID): The segmenting principle suggest that providing learners with opportunities to pause and process the information before continuing to the next step helps them learn more deeply [107]. This could be achieved by dividing a multimedia message into learner-paced chunks rather than presenting the information as a continuous unit [104]. All comic-based works present their content in individual segments, pages, or chapters.

4.2.3 Tabletop Games

Learning that take places in group environments fosters discussion and interaction. Tabletop games accommodate co-operative learning through multi-player security themed card or board games that encourage discussion among players in social settings. Security advice is uncovered in the context of players' actions.

The Simulation Principle (PT): Simulations provide the means to observe cause-and-effect relationships in users' behaviour. Security-themed tabletop games simulate security experiences by incorporating them into gameplay. In the Smells Phishy board game [13], players are exposed to simulated phishing risks in the context of online shopping. Players are motivated to link the game security concepts to their real life experiences and share their stories with other players.



There's a service on HatNet called SatView, that lets you access real-time video feeds from satellites. You could use this to scan the ground for duplicates.

Figure 4.3: The Watchers [137] board game component (left), and the app component that auguments gameplay (right).

The Conceptual/Procedural Principle (ID): Instruction that focuses on building a mental representation of an idea builds conceptual knowledge, while instruction that focuses on the correct steps to solve a problem or complete a task builds procedural knowledge [36]. Research suggests that there is a causal relationship between conceptual and procedural knowledge. For example, a study [145] examining the relations between children's conceptual understanding and procedures for solving mathematical equivalence problems found that conceptual knowledge led to increased understanding and transfer of a correct procedure, while procedural knowledge led to increased conceptual understanding. The two types of instructions are therefore mutually supportive in learning. Several security-themed card games enable users to play as hackers to build conceptual and procedure knowledge. In Ctrl-Alt-Hack [45] and [d0x3d!] [69], users with technical backgrounds play as white-hat hackers. They gain procedural knowledge by learning about attack techniques and gain conceptual knowledge of the challenges and needs in computer security so that they can be informed technology builders and consumers.

The Reflection Principle (ID): Learning increases if the learner is given opportunities to reflect on what they have learned [128]. Reflection is a form of mental processing used to fulfill a purpose or to achieve some anticipated outcome to further the processing of knowledge and understanding [120]. In The Watchers computer augmented board game [137], board gameplay is guided by an app with animation and interactive features that give feedback about the consequences of the players' actions (Figure 4.3 shows examples of the board game component and the app component).

Interactions between choices, actions and consequences cause players to reflect on the relationship between actions and outcomes.

4.2.4 Visualizations

Visualizations utilize the human visual system's ability to see patterns and trends to enhance cognition, and are faster to consume than textual information [23]. Retention of visual information is supported by the picture superiority effect [119], which states that people remember images better than text. Successful manipulation of information and data can be achieved through information design, where the goal is to portray information or data effectively and efficiently for people to understand. In computer security, visualized security information enhanced risk communication and safe behaviour [135], increased comprehension [90], and provided better retention than text-only security information [188].

The Reduction Principle (PT): A system that reduces user effort helps users perform the target behaviour and may increase the cost/benefit ratio of a behaviour. This principle is highly relevant because many users find online privacy and security difficult to understand and manage [182]. A commonly applied approach to overcome this challenge is to simplify information so that it is easier to learn and understand. In one work, Kelley et al. [90] applied design elements from nutrition, warnings, energy labeling, and banking privacy notifications to security policies to improve their comprehensibility. Camp [87] proposed metaphors to support security mental models. Several studies [135, 186–188] showed that users learned more effectively from analogies and metaphors. In the design of firewall warnings, Raja et al. [135] found that a personal firewall visualized based on a physical security metaphor facilitated better comprehension, risk communication, and increased the likelihood of safe behaviour than existing firewall warning messages. Our prior studies [186–188] showed that infographics with visual metaphors (see Figure 4.4) are more effective at improving the comprehensibility and retention of security advice compared to text-only information in several security areas. In information visualization, we created GeoPhisher [190] to visualize textual data from a large phishing blacklist database to quickly generate phishing URL patterns on a map based on time, location, and the targeted brand.

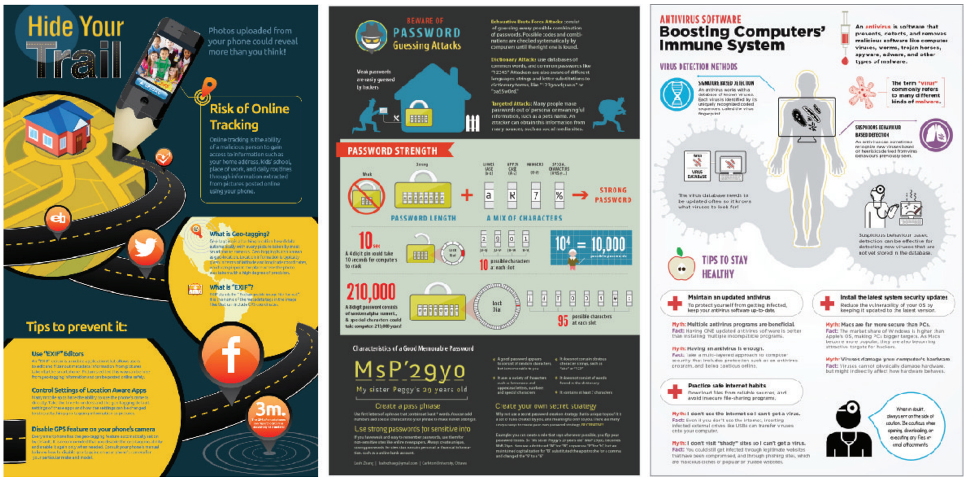
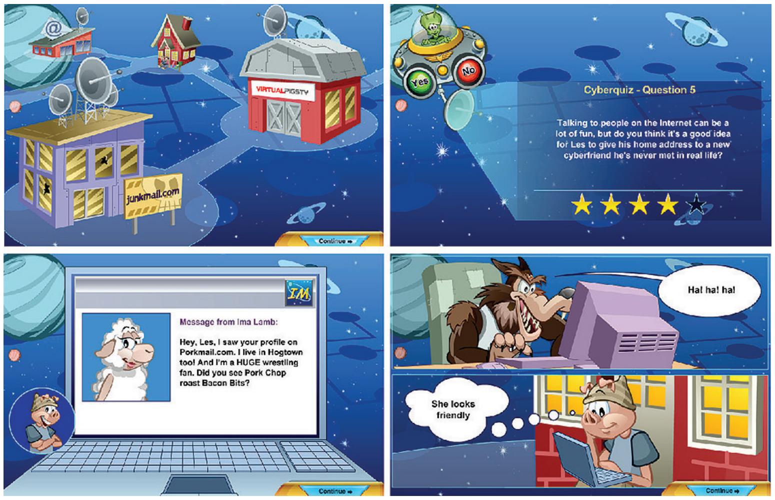


Figure 4.4: Security Infographics using visual metaphors to illustrate three security concepts: Hide your digital trail online [114] (left), passwords are like locks [187] (centre), and antivirus software strengthens computers' immune system [188] (right).

The Signalling Principle (ID): Deeper learning could be achieved when cues are added to highlight essential content and call to attention the important material in the lesson [104]. Signalling could be applied to text (e.g., bold, highlight, underline) and visual content (e.g., colours, arrows, spotlight). For example, in computer security dialogs design, Bravo-Lillo et al. [20] used visual and inhibitive cues to prevent potentially-dangerous behaviours and redirect users' attention to salient information. Mayer [105] suggests that the signalling principle may be applied most strongly when it is used sparingly rather than excessively. Signalling is used to emphasize important information in privacy and security education, such as in the design of privacy labels [90] and information graphics [186–188] to increase comprehension and enable users to discover information quickly and accurately.

4.2.5 Learning Modules

A learning module is an education tool that guides learners through educational content made up of chunks of information, usually presented in a sequential manner [148]. A learning module could include text, images, audio, video, animation, or other types of multimedia. Some learning modules aim to increase learning motivation and engagement by using gamification [148], which is the use of game design elements in



Cyberquiz - Question 5

Talking to people on the Internet can be a lot of fun, but do you think it's a good idea for Les to give his home address to a new cyberfriend he's never met in real life?

Message from Ima Lamb:

Hey, Les, I saw your profile on Porkmail.com. I live in Hogtown too! And I'm a HUGE wrestling fan. Did you see Pork Chop roast Bacon Bits?

Figure 4.5: The online predator segment from the learning module Privacy Playground: The adventure of the three CyberPigs [112].

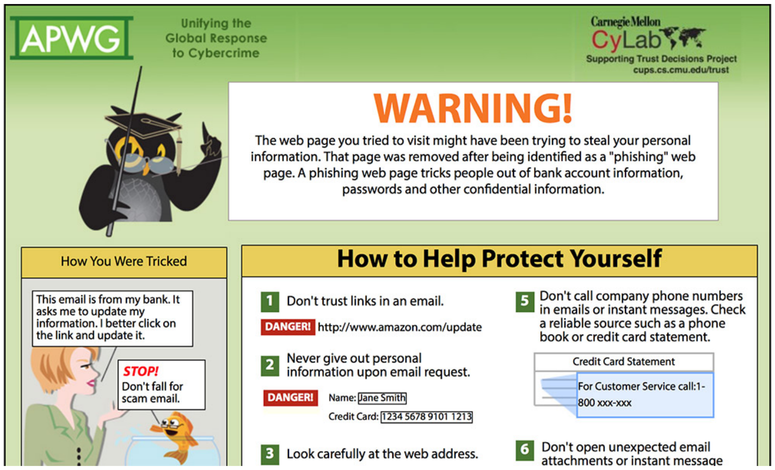
non-game contexts [46]. The following principles are commonly used in the design of learning modules.

The Multimedia Principle: Multimedia refers to the use of multiple media types in the education material, such as images, text, sound, and animation. Paivio's dual coding theory [34] suggests that graphics, text, and audio are coded into memory differently. People process text and audio in their phonetic working memory, while images are encoded in visual working memory. The theory implies that the combination of related text and images helps to enhance comprehension, and increases long-term memory. Graphics could involve a range of visual media such as illustrations, photographs, animation or video. For example, in Privacy Playground [112] (See Figure 4.5, children interact with an animated story about the three CyberPigs as they encounter various privacy and online safety situations and answer quiz questions. Research suggests that multimedia supported environments help students engage in learning, and result in superior learning outcomes than text alone approaches [106]. All of the learning modules in Table 4.6 use the multimedia principle.

The Tunnelling Principle (PT): The tunnelling principle states that a system that guides users through a process or experience enables persuasion in the process. We see examples of tunnelling in all of the learning modules by Media Smarts. For example, in Privacy Pirates [111], children answer quiz questions about privacy and personal information in a sequential manner and are rewarded with map pieces for correct answers leading to a pirate treasure.

The Immediate Feedback Principle (ID): Immediate feedback might include praise, advice, and evaluation that could help the learner to assess how they are doing. Researchers (e.g., [4, 151]) found that immediate feedback provides efficient guidance in learning. Positive feedback such as giving praise and reward is a form of conditioning that reinforces a target behaviour [58]. However, Hattie and Timperley [77] stress the importance of avoiding ambiguous feedback like "great job!" or "not quite there yet" because they do not provide any insight into what was done right or wrong, and how it could be corrected. Feedback should supply learners with concrete information to help them improve. In Co-Co's AdverSmarts [110], the cereal character Co-Co Crunch provides children with positive feedback like "good job!" or "way to go!", and followed by dialogue to explain the consequences of the players' selection.

The Socialization Principle (ID): The instructional design principle of socialization (also known as personalization) addresses the concept of "attributing social characteristics to the user interface" rather than "customizing on a per user basis" as the term "personalization" is commonly used in persuasive technology. The theory of Media Equation [140] states that people respond to computers in a similar way to how they respond to other people through social conventions. Learners engage better with educational content when the message is delivered in conversational style rather than formal language [35]. It is also evident that the use of a pedagogical character that offers instructional advice can improve learning [104], since people pay more attention to someone who is speaking directly to them by evoking a conversation [35]. Pedagogical characters can be human or non-human, realistically depicted or cartoon-style, and represented visually or verbally. They could effectively narrate the lesson and put it in the context of a story, demonstrate the concepts, and direct visual attention to the key features on the screen [7, 108, 121]. For example, users are guided by a cereal character, Co-Co Crunch in Co-Co's AdverSmarts [110], a robot character in Click if you Agree [109], and a pirate character in Privacy Pirates [111]. These pedagogical characters converse in friendly, first-person language. They provide children with immediate feedback and encourage them to continue.



APWG

Unifying the Global Response to Cybercrime

Carnegie Mellon CyLab

Supporting Trust Decisions Project
cups.cs.cmu.edu/trust

WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank. It asks me to update my information. I better click on the link and update it.

STOP! Don't fall for scam email.

How to Help Protect Yourself

1 Don't trust links in an email.

DANGER! http://www.amazon.com/update

2 Never give out personal information upon email request.

DANGER! Name: Jane Smith
Credit Card: 1234 5678 9101 1213

3 Look carefully at the web address.

5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

Credit Card Statement
For Customer Service call:1-800 xxx-xxx

6 Don't open unexpected email attachments or instant message

Figure 4.6: Users are redirected to this phishing advice webpage from APWG's Phishing Education Landing Page program [5] after they have clicked on a phishing link.

4.2.6 "Just-In-Time" Systems

Learning is most effective when it takes place just-in-time, at the most teachable moment [102]. A "teachable moment" in education refers to the time at which learning a particular topic or idea becomes possible or easiest [78]. This type of system is explored in anti-phishing education, where a teachable moment is created when users fall for a real or simulated phishing attack. Although the approach is effective at getting users to pay attention to security information, regulatory and ethical considerations should be addressed, such controlling how the simulated phishing emails are sent and sensitivities toward the invasion of the recipients' privacy. Several persuasive principles influence the design of just-in-time systems.

The Suggestion Principle (PT): A system that provide users with appropriate suggestions for action could persuade them to carry out a behaviour. Anti-phishing education systems provide users with suggestions and tips for the correct behaviour when they are faced with security-related decisions. For example, after users fall for a phishing communication in PhishGuru [94] or the Anti-Phishing Working Group's (APWG) phishing education landing page program [5], they are re-directed to educational webpages (See APWG's example in Figure 4.6) that provide step-by-step advice on phishing prevention.

The Tailoring Principle (PT): Information is more persuasive if it is tailored based on the potential needs, interests, usage context, or other considerations relevant to a user group. The PhishGuru phishing email training system, for example, is suitable to training users in an organizational context [94]. Adult privacy and security education is generally tailored to non-expert users to augment their limited technical understanding, or is designed to appeal to users with technical backgrounds to enhance their security awareness. Beyond these broad classifications, however, we found that few systems explicitly expressed considerations for other factors within these user groups such as age, gender, culture, and usage context. In children's privacy and security education, we found more specialization in tailoring material according to age groups to accommodate for children's developmental needs. For example, education materials designed for younger children frequently uses colourful cartoon style with animation, sounds, and voice narration to stimulate children's senses to engage them in the lesson.

The Monitoring Principle (PT): Monitoring and reporting users' performance using a system (either self-monitored or under surveillance) could help them see behavioural patterns of harmful actions. This creates an opportunity to educate users about what behaviours need to be adjusted for better security. For example, the Privacy Leaks app [9] monitors the frequency and destination of users' shared data. A visual summary of the shared information and just-in-time notifications are provided to warn users about potential data leaks. Such tool helps to correct misconceptions between what users think is happening on their devices and the actual events.

The Personalization Principle (PT): The personalization principle states that a system offering personalized content has a greater capability for persuasion. Personalized advice relating to users' actions and usage context could help them pay attention to security information and understand the causality of their actions. The Privacy Leaks app [9] personalizes privacy disclosure data based on the apps and services the user has installed on his or her personal smartphone and what data the apps collect from the user.

4.3 Discussion

We explored persuasive technology and instructional design principles used in privacy and security educational material for children. Although these design principles seem appropriate for children, their application may be more challenging for children than for adults. On a high level, the main differences we found between adults' and children's privacy and security education are simplicity and developmental fit.

4.3.1 Simplicity

Reduction is the most commonly applied principle in privacy and security education to reduce cognitive load. The concept of simplicity is even more important to consider when designing for children due to their limited information processing abilities, attention, and working memory abilities [84].

In general, designers should strive to limit the number of user interface components so they can be easily perceived by children, and written language should be kept to a minimum to fit within children's moderate vocabulary, and supplemented with images or sound [84]. In our literature review, children's education material has less text and more multimedia support than work created for adults. In some systems (e.g., Privacy Playground [112]), children are not required to read at all because any onscreen text is overlaid with voice narration. However, research [35] suggests that including both text and audio that reads the text is redundant and could hurt learning. They recommend using text or voice narration, but not both [35].

The *segmenting* principle is used in all children's work reviewed to accommodate for children's limited ability to understand hierarchies and to focus on no more than one characteristic at a time [130,132]. Breaking up complex tasks or information into simpler chunks may help make the learning material more accessible for children.

Tunnelling techniques are sometimes used in adult content to keep users on track and prevent them from diverging from the material and making errors, but these do not allow exploration, which is a primary mode of learning for children [84]. We found that tunnelling is used often in children's learning modules. A major drawback is that these modules do not allow children to skip ahead or backtrack if they wish to explore or correct a mistake. Although tunnelling techniques may be appropriate for children in some situations, they should allow certain levels of flexibility that are compatible with children's high-level goals such as entertainment and exploration [84].

4.3.2 Developmental Fit

Developmental fit refers to children's ability to understand how to use a technology in a positive, constructive way [84]. This requirement may put various constraints on design. It is not surprising that children's education work is more age-sensitive than adults', which has a more generalized target audience. This is due to variations in children's developing cognitive abilities, their prior experiences, and the social and physical environments they live in; a small age gap of 2 to 3 years may result in significant differences in children's ability and experience [84], but variability is reduced in adults. Therefore, we found that it is common to apply the *tailoring* principle to appeal to children of a specific age, particularly when the educational system aims to simulate situations or the environment of that age group.

Discussions of privacy and security topics need to be relevant and age-appropriate for children, both in terms of technical details and possible protective actions. In addition, the educational system needs to be accessible for children. For example, a user interface with multiple menus and precise controls is not a good developmental fit for children. Designers of children's technology could apply principles such as *reduction, tailoring, segmenting, contiguity,* and *signalling* to make learning tasks easier to do. *Immediate feedback* and the ability to reverse errors are also important factors. The principles invite exploration and give children the option to undo errors. Children need appropriate feedback to clearly perceive the consequences of their interactions as quickly as possible and to understand what the technology is doing [84].

Personalization in children's education could help to make the lessons more relatable to individual children. We found that very few adults' systems and none of the children's systems allowed customization. We believe that children could benefit from some level of customization, such as the ability to select characters based on their gender. *Social cues* are also important for children. Since children's development and experiences often involve caregivers and teachers, it is sensible to consider their involvement in children's learning. Principles like *social cues* and *socialization* could be used to support this need in the user interface. Designers could provide children with positive feedback from pedagogical characters similar to caregivers and teachers as a form of *conditioning.* it is also possible to involve caregivers and teachers in the use of the educational system.

Children's systems rely more heavily on multimedia features for engagement compared to systems created for adults. These may include combinations of text, images, animation, sounds, and voice narration. However, researchers caution that using an excess of multimedia in education material could decrease learning, distract learners from key instructional points, disrupt their ability to mentally organize information, and activate irrelevant prior knowledge that increases the cognitive load [48, 76]. Therefore, multimedia should be used to support learning goals, rather than used extraneously. Visual design considerations for children, such as the use of bright colours, large icons and menus so children can easily click on them, and reducing visual complexity should also be addressed.

4.4 Gap Analysis

The results of this literature review open new avenues for future research and serve as a source of hypothesis for further studies on privacy and security educational work for children. Even though many educational tools are currently available, our literature review revealed that many systems were designed for adult users, and few were designed for children (particularly young children). Children's educational tools were rarely evaluated, as identified in our analysis in Table 4.7. We specifically identified simplicity and developmental fit as important design considerations for children. Even though we analyzed prior work based on established design principles, the use of the principles was usually not explicitly stated by their original authors, nor formally incorporated in a research-drive design process. Since many children's educational tools were not empirically evaluated, we cannot assess their effectiveness. Further, qualitative research is needed to study what privacy and security mean to children, so that the design of educational materials can better match conceptual models to children's existing mental models. Additionally, qualitative research is needed to identify the common conceptions and misunderstanding that children have about online privacy and security, so that educational material can be targeted to correct them. Researchers should also take into consideration the public perceptions and individual family's preferences for the type of privacy and security information and the age-appropriateness for exposing children to this information. Without an understanding of privacy and security from children's perspective, a theoretical background for design, and evaluations for effectiveness, we cannot ascertain that education material have any real impact on children's actions to protect their privacy and security online.

4.5 Research Roadmap

We begin our research in the next chapter with a preliminary study of our work, Secure Comics about mobile online privacy, with children aged 11 to 13 to test its effectiveness at improving children's privacy knowledge and behaviour, and to study whether interactive visual narratives like comics are an effective format for engaging children in privacy and security information. Next, we conducted a qualitative study of children's privacy models and perceptions of online threats with children aged 7 to 11 to gain an understanding of online privacy from their perspective. These perspectives were taken from the home context, where children's daily interaction with technology often involved parents, siblings, and friends. Our results reveal several unique challenges that children and their caregivers face in managing children's online privacy, and differences in the threats that they perceive might harm children. Our findings from these two studies established the foundation for designing privacy and security multimedia learning tools for children. We identified that a more significant gap in knowledge and a high level of concern from parents existed for the younger children and chose to focus subsequent efforts on educational material for them. We designed the interactive ebook, Cyberheroes, and evaluated it with children 7 to 9 years old. Interactive ebooks have the potential to increase children's engagement [88], to support personalized learning [85], and to support children's learning by adult instruction [153]. The goal of the design and evaluation process is to gain an understanding of the effectiveness of our prototypes at improving children's knowledge and behaviour, and to assess whether persuasive technology and instructional design principles are effective for designing children's privacy and security educational tools.

Chapter 5

Secure Comics About Mobile Online Privacy: Design

Secure Comics[1] is a three-part educational digital interactive comic book created by us that had positive effects on adult users' understanding of security and privacy topics, and security and privacy management behaviour [189]. Figure 5.1 shows the landing screen for the Secure Comics series. The first two parts on the topics of passwords and malware were created and tested as part of Zhang-Kennedy's Masters Thesis [187, 188]. The third part on the topic of mobile online privacy was conceptualized, designed, implemented, and tested with both adults and children during this PhD research. Screenshots of the new privacy comic are included in Appendix A.

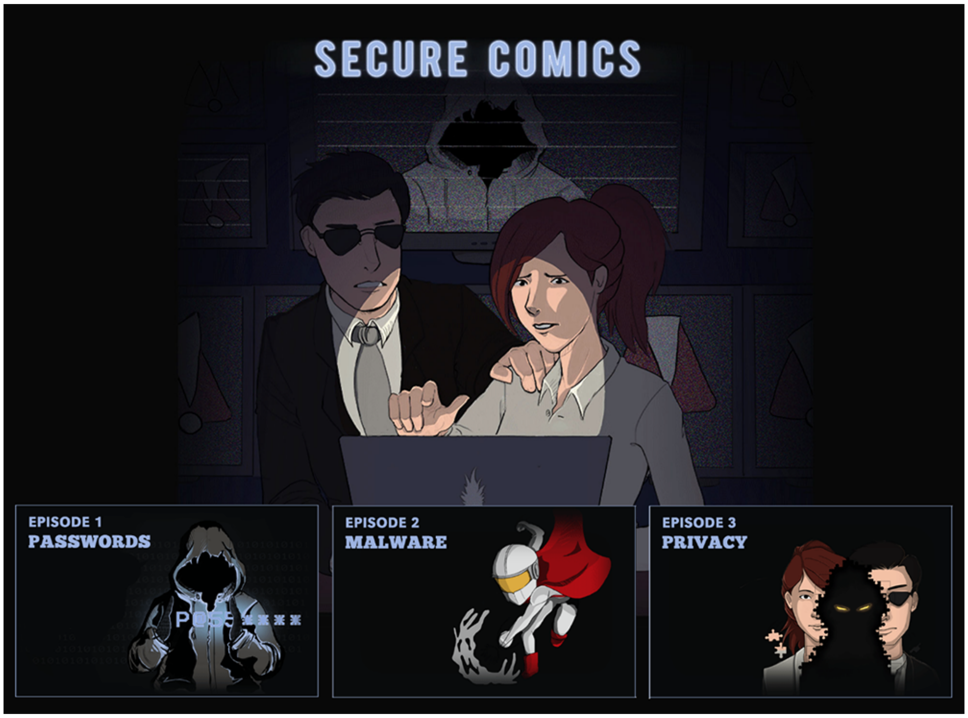


Figure 5.1: Landing screen for the three-part Secure Comics series.

[1] Secure Comics is available online at http://www.versipass.com/edusec/securecomics and in the Apple Store

We used a process-driven design approach adapted from the ADDIE instructional design model [74]. ADDIE is a five-phase iterative model that stands for Analyze, Design, Develop, Implement, and Evaluate. It was first introduced as an instructional systems development (ISD) program for military service training [18], and has evolved into a general iterative process applicable to many areas of instructional design. For example, ADDIE is used to design learning activities for online learners in the virtual world of the game Second Life [176].

Figure 5.2 illustrates the ADDIE process. The designer first gathers information about the target audience, project objectives, constraints, and desired learning outcomes during the *analyze* phase. Then, lesson content is planned to meet the desired behavioural outcomes in the *design* phase. These may include low-fidelity prototypes and concepts so that they can be iterated quickly at low cost. During *development*, content is assembled in storyboards and sample graphics are created to get feedback and iterate the designs. The content is then *implemented* and error checked before it is evaluated to monitor periodic learning outcomes. ADDIE is a dynamic iterative process. Therefore, formal (e.g., user studies) and informal (e.g., constructive feedback) *evaluations* may be involved at any stage of the process.

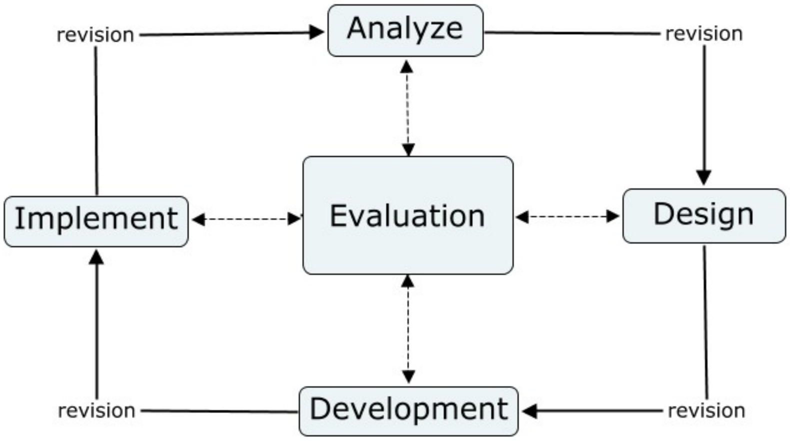


Figure 5.2: The ADDIE instructional design process. Diagram adapted from Wikimedia [37]

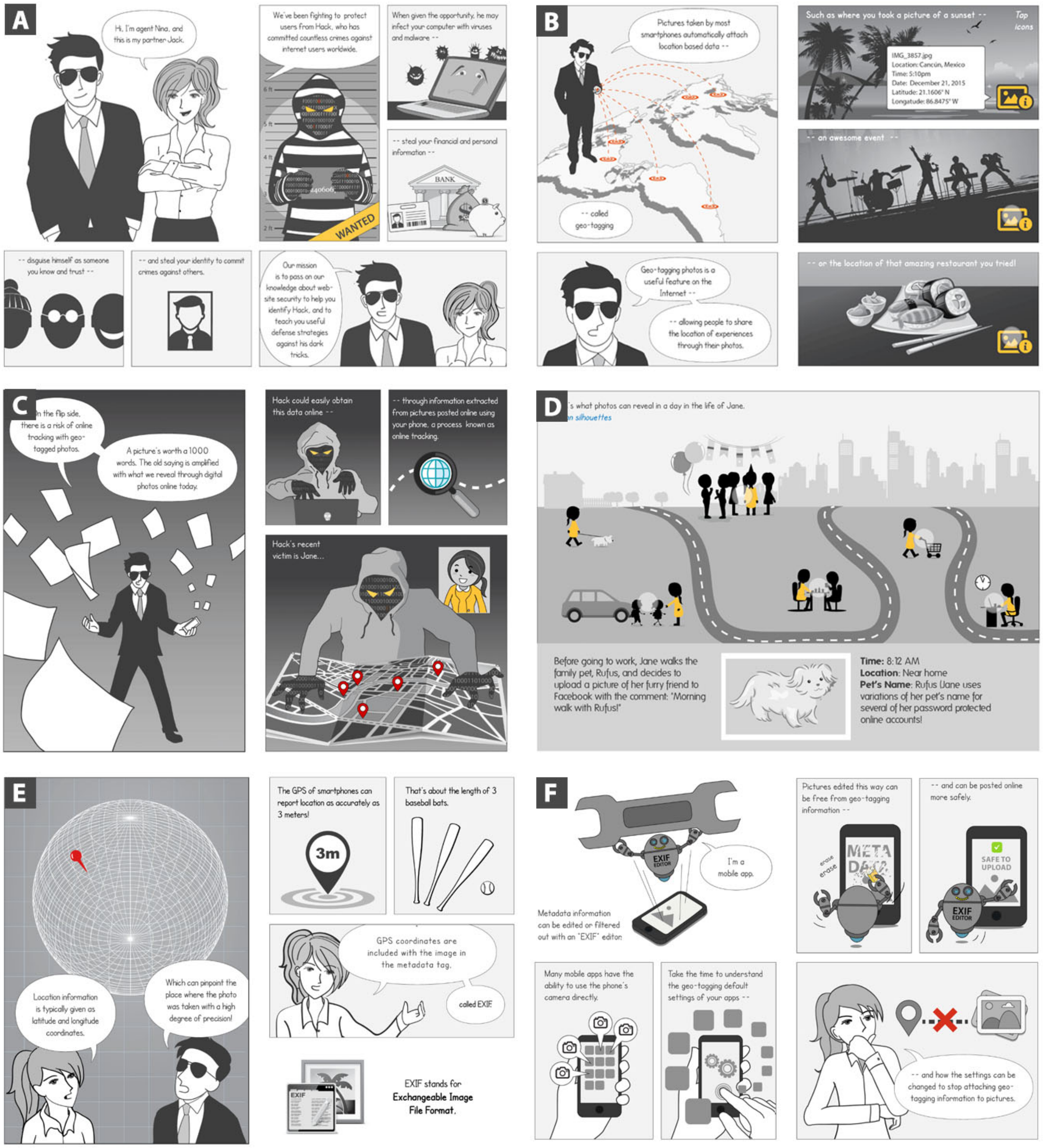

A
Hi, I'm agent Nina, and this is my partner Jack.
We've been fighting to protect users from Hack, who has committed countless crimes against internet users worldwide.
WANTED
When given the opportunity, he may infect your computer with viruses and malware --
-- steal your financial and personal information --
BANK
-- disguise himself as someone you know and trust --
-- and steal your identity to commit crimes against others.
Our mission is to pass on our knowledge about web-site security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.
B
Pictures taken by most smartphones automatically attach location based data --
-- called geo-tagging
Such as where you took a picture of a sunset --
Tap icons
IMG_3857.jpg
Location: Cancún, Mexico
Time: 5:10pm
Date: December 21, 2015
Latitude: 21.1606° N
Longatude: 86.8475° W
-- an awesome event --
Geo-tagging photos is a useful feature on the Internet --
-- allowing people to share the location of experiences through their photos.
-- or the location of that amazing restaurant you tried!
C
n the flip side, there is a risk of online tracking with geo-tagged photos.
A picture's worth a 1000 words. The old saying is amplified with what we reveal through digital photos online today.
Hack could easily obtain this data online --
-- through information extracted from pictures posted online using your phone, a process known as online tracking.
Hack's recent victim is Jane...
D
's what photos can reveal in a day in the life of Jane.
n silhouettes
Before going to work, Jane walks the family pet, Rufus, and decides to upload a picture of her furry friend to Facebook with the comment: "Morning walk with Rufus!"
Time: 8:12 AM
Location: Near home
Pet's Name: Rufus (Jane uses variations of her pet's name for several of her password protected online accounts!
E
Location information is typically given as latitude and longitude coordinates.
Which can pinpoint the place where the photo was taken with a high degree of precision!
The GPS of smartphones can report location as accurately as 3 meters!
3m
That's about the length of 3 baseball bats.
GPS coordinates are included with the image in the metadata tag,
called EXIF.
EXIF
EXIF stands for Exchangeable Image File Format.
F
EXIF EDITOR
I'm a mobile app.
Metadata information can be edited or filtered out with an "EXIF" editor.
Pictures edited this way can be free from geo-tagging information --
META DATA
erase erase
-- and can be posted online more safely.
SAFE TO UPLOAD
Many mobile apps have the ability to use the phone's camera directly.
Take the time to understand the geo-tagging default settings of your apps --
-- and how the settings can be changed to stop attaching geo-tagging information to pictures.

Figure 5.3: Six pages from Secure Comics' ten-page privacy chapter. B & D have interactive features. A) Intro; B) Geotagging (with interactive picture icons); C) Online tracking; D) A day in the life of Jane (with interactive activities map). E) GPS Accuracy; F) Removing Metadata. Note: navigation is cropped from the screens

PT & ID Principles	Used	Implementation
Reduction	◐	We leveraged users' familiarity with the "trail" metaphor to communicate about online tracking. Each panel of the comic strategically breaks down privacy concepts into manageable learning chunks.
Tunneling		
Personalization		
Conditioning	◐	Users receive praise like "good work, thanks for your help!" or "good job!" followed by constructive feedback for answering questions in the quiz mini-game.
Suggestion	◐	Jack and Nina suggest best-practices for protecting online privacy after users learn about online tracking.
Tailoring		
Social Cues	●	Jack and Nina guide users through the lesson content and motivate them along the way. The "good guys" are designed with a sense of humour to make them well-rounded and interesting.
Simulation		
Monitoring		
Rehearsal		
Procedural Rhetoric	◐	In "A day in the life of Jane", shown in Figure 5.3C, users interact with Jane's various daily activities and gradually witness how seemingly harmless interactions could reveal sensitive information.
Segmenting	●	The comic is segmented into sections and pages to enable users to progress at their own pace. Users press a forward or backward button to move ahead or backtrack.
Contiguity	●	Graphics are designed to complement text explanations and facilitate comprehension.
Reflection	◐	Interactive components in the comic cue reflection of the lesson content by concealing answers under graphics that are activated on mouseover.
Immediate Feedback	◐	Users receive constructive immediate feedback in the mini-quiz game about why their choices are correct or incorrect.
Narrative	●	The story revolves around agents Jack and Nina as they tackle new security crimes committed by Hack.
Signaling	●	Various visual treatments (e.g., bold, colour-highlighting) are applied to text and graphical information to direct the learners' attention.
Socialization	●	Jack and Nina guide users through the lesson and motivate users along the way. They use a positive conversational language when speaking to users.
Multimedia	●	Ideas are expressed through text, images, and interactive elements to engage users.
Conceptual-Procedural	●	The comic helps users develop conceptual knowledge by building mental models through metaphors and telling analogies (e.g., 'trail' metaphor), and provide procedural examples to help reinforce the concepts (e.g., how to prevent online tracking.

Table 5.1: Design principles implemented in Secure Comics. ● = strongly uses the principle; ◐ = weakly uses the principle; *no circle* = does not use the principle.

5.1 Analysis Phase

Our previous work on evaluating metaphors for risk communication of the same privacy concepts using infographic posters [115] found that participants responded most positively to the “trail” metaphor because it alludes to tracking, where attackers could obtain the digital trail left online by users through geo-tagging and shared location information. Using this work as a starting point, we conceptualized the privacy comic based on the “trail” theme..

5.1.1 Educational Goals

The goal of the privacy chapter was to familiarize users with the concepts of geo-tagging and online tracking, and to provide actionable advice on how to prevent the disclosure of location-based information. We assumed little to no knowledge about these topics from our users, so the comic should be easy to understand. Users should be able to recall information they learned from the comic, apply the lessons to different situations, and distinguish relationships between certain actions and consequences. To facilitate these goals, the comic first set the scene, then explained details of the risks. Advice about the corresponding secure actions immediately followed to justify their need. Lastly, users tested their knowledge in a mini quiz game. Our rationale is that if users understood the risk and had means to act, it would increase the likelihood of desirable behaviour. The comic focused on the following topics. Educational messages are followed by recommendation of what users should do to mitigate the risks.

- Geotagging: Sharing photos online could reveal sensitive location-based information about users, their family, and their friends. Geo-tagging automatically attaches metadata to photos taken with smartphones with personal information such as the exact location, date, and time. Metadata information could be removed using EXIF (Exchangeable Image File Format) editors, a type of mobile app that filters out metadata information from photos so they could be posted online more safely.

- Online tracking: Location information could be maliciously used for identity theft, stalking, or behavioural advertising. Users often reveal sensitive information about themselves or others without their explicit knowledge due to geo-tagging. Photo content, user comments, and tagged photos of other people on social media could also real sensitive information. Users should avoid including personal and location information of themselves and others when posting photos or writing comments online.

- GPS: Smartphones equipped with GPS are capable of tracking and transmitting users' location. GPS uses latitude and longitude coordinates to pinpoint the location of the photo with great accuracy. GPS could be disabled to prevent geo-tagging and only enabled when it is necessary.

The advice included in the comic provided the targets for assessing children's privacy behaviour based on their responses to situation-based scenarios in Chapter 6. For example, one of the scenarios we used was "suppose you want to sign up for a new social media account. It requests that you upload a picture of yourself with your address, phone number, and email address so other members of the website can contact you." Children were asked what they would do in the given situation, and how the situation might affect their privacy and others' privacy. Children were provided with visual aids of the screens and posts. The target behaviour for this scenario was to not sign up, or press the "skip" button to signup without providing the information. This is because the address, phone number and email address could be collected and used for spam and other purposes. The disclosure of the information could affect everyone living at the same address.

5.1.2 Entertainment Goals

Our second goal was to make the comic fun and entertaining to read. Our design approach embeds security learning within a fun activity – interacting with a comic book. Comics convey engaging stories, are fun to read, and have large readerships of all ages. Our comic design leverages the media's power to express ideas through images, text, and narrative storytelling, but also explores modern media techniques like graphic design and interactive features to engage users. Our goal was to create highly attractive graphics, likeable characters, and an exciting narrative to maximize appeal to the audience.

5.2 Design Phase

5.2.1 Secure Comics overview

Narrative: Secure Comics have evolved into a three-part series. where each part is an Internet crime case committed by Hack that agents Jack and Nina try to solve. Part one of the comic focuses on passwords, part two on malware, and part three on mobile online privacy. In the mobile online privacy chapter, Agent Jack takes a picture and uploads it online. He admits that taking pictures with smartphones is fun and convenient, but cautions that location-based data are automatically tagged to photos in a process called geo-tagging. The cyber-villain Hack is able to extract many types of user information from pictures. Indeed, his recent victim is a woman named Jane, who revealed many secrets through photos posted online (See Figures 5.3, C & D). Nina and Jack then explain online tracking and how to prevent it.

Characters: The main characters, Jack and Nina, are cyber-detectives who solve computer security crimes to protect the public from the cyber-villain "Hack". Jack and Nina act as mentors to teach users about various risks and protection strategies. Minor characters are introduced in the comic to support the overarching narrative.

5.2.2 Design Principles

We applied design principles from persuasive technology (PT) and instructional design (ID) introduced in Chapter 4 to design Secure Comics. Some principles were used throughout the comic, while others were used in certain parts of the comic. For example, the ID principle of *contiguity* was widely applied to the design of the comic, while the PT principle of *conditioning* was used specifically in the design of the interactive quiz game. A summary of principles and how they were used in Secure Comics is provided in Table 5.1. Principles that were applied throughout the comic are labeled as "strongly used" (i.e., full circle), and principles that were applied to certain parts of the comic are labeled as "weakly used" (i.e., half circle).

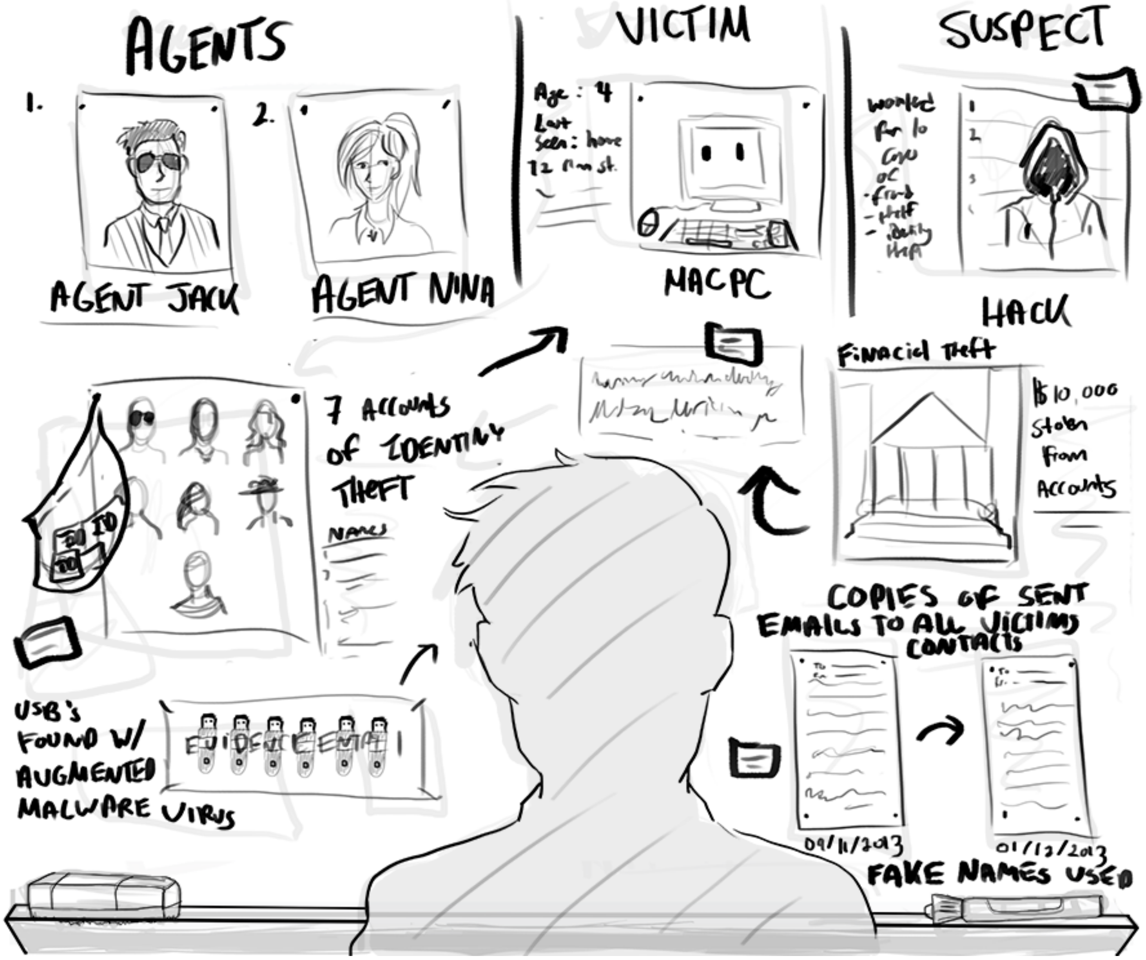


Figure 5.4: One of the early concept sketches for Secure Comics.

Fogg's *Functional Triad* identifies *media* as one way that PT can operate to change behaviour [58] — to persuade people by allowing them to explore cause-and-effect relationships, or to provide them with vicarious experiences that motivate or help people to rehearse a behaviour. Work in usable security that educates users about phishing threats (e.g., [156]), privacy policies (e.g., [90]), and data leaks on smartphones (e.g., [9]) has exemplified that good instructional design increases users' comprehension of privacy and security information, and media can have positive effects on motivating positive behaviour. Other work successfully applied PT theory in authentication systems to persuade users to create stronger passwords (e.g., [26, 168, 169]). In one work, Srikwan and Jakobsson [165] suggest that presenting serious topics like computer security as a comic could help users to overcome the "intimidation factor" associated with learning technical topics.

Secure Comics function as media and use PT principles to persuade users toward secure and privacy-conscious behaviour, and apply ID principles to make the information easier to understand. For example, to reduce the cognitive load and increase comprehension, we used a juxtaposition of *multimedia* including images, text and interactive elements. The graphics are designed to complement the text explanations and to facilitate comprehension by illustrating connections between concepts or providing visual examples. For instance, when explaining the accuracy of GPS coordinates in Figure 5.3, E, Jack and Nina demonstrate using concrete visual examples. The comic makes learning easy to do because complex security topics are broken down into manageable learning steps to reduce the cognitive load using the *reduction* principle. *Segmenting* is applied to cover one security topic per issue as Agents Jack and Nina tackle a new security crime committed by Hack. Each comic is divided into sections and pages to enable users to progress at their own pace.

Secure Comics use gender-inclusive pedagogical agents and symbolic characters to appeal to readers' emotions. Characters are both male and female to appeal to learners of both genders, and are designed to embody *social cues* and *socialization* characteristics. For example, Agents Jack and Nina use positive conversational language to speak to users about various security concepts. They address readers in a friendly, first person style, such as using the words "I" and "you". The characters provide encouragement to users by providing *immediate feedback* and *conditioning.* For example, when users correctly answer a question in the quiz game, a character gives praise such as "good work", or "that's right!", followed by an explanation of what they answered right. When they answer incorrectly, the character provide cautionary feedback such as "are your sure?" or "Uh-oh", followed by a constructive explanation of the correct response. Users receive *suggestions* of privacy and security advice from the characters after learning about the threats to justify the need for secure actions. Characters in Secure Comics are symbolically designed to appeal to readers' emotions. For example, the supervillain character, Hack, has a dark and mysterious physical appearance (See Figure 5.3, A and C). His piercing and menacing eyes glow over a face that is always shadowed under a hood. These characteristics make Hack appear uncanny and untrustworthy. Some characters personify abstract concepts to give them a symbolic physical and emotion presence. For example, we portrayed the "EXIF editor" as a friendly robot mechanic who fixes picture files by removing metadata (See Figure 5.3, F).

The comics help users develop *conceptual* knowledge by building mental models through metaphors and analogies, then provide *procedural* examples to help reinforce the concepts. Where appropriate, we incorporated interactive elements into the security lessons in the narrative to help to show cause and effect relationships to enable users to interact and reflect on the lessons. For example, after comparing the concept of online tracking to physical tracking in the privacy comic using the "trail" metaphors, we included an interactive page: "A day in the life of Jane" (shown in Figure 5.3, D) to illustrate the step-by-step process of how online tracking could take place. As users interact with Jane's various daily activities, they procedurally witness how this ordinary person's seemingly harmless interactions could reveal sensitive information. Jane's story aims to reinforce *conceptual* knowledge about online tracking. Immediately afterwards, users gain *procedural* knowledge about how to prevent online tracking.

5.3 Development Phase

5.3.1 Content Development

During the early development, hand-drawn concept sketches were created (see Figure 5.4). We drafted a written script and planned dialogues between the characters based on this narrative. Next, storyboards were developed and iterated based on constructive feedback from privacy and security researchers in our lab, and other graphic designers. Figure 5.5 shows an example of one of the early storyboards and the final version. In the storyboard, agent Nina appears in the photograph. We later changed the character to a child to further highlight the risks.

Interactive Features: We structured the privacy comic to include four sections: introduction to online privacy, what is geo-tagging, how online tracking works, how to prevent online tracking and geo-tagging, and a mini review quiz to reinforce the

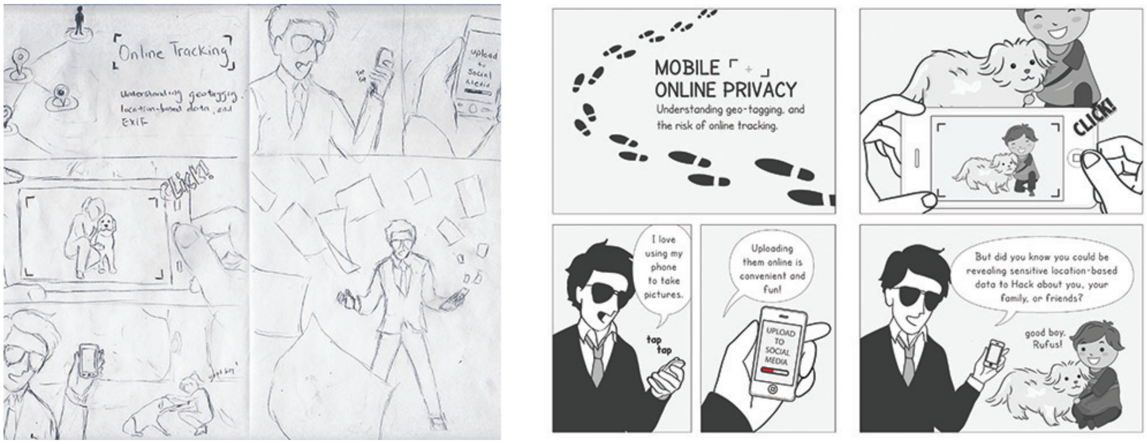

Online Tracking
Understanding geotagging location-based data, and EXIF
upload to Social media
CLICK!
MOBILE ONLINE PRIVACY
Understanding geo-tagging, and the risk of online tracking.
CLICK!
I love using my phone to take pictures.
tap tap
Uploading them online is convenient and fun!
UPLOAD TO SOCIAL MEDIA
But did you know you could be revealing sensitive location-based data to Hack about you, your family, or friends?
good boy, Rufus!

Figure 5.5: An early storyboard (left) and its final screen (right).

concepts. Out of the ten screens, three contained interactive features to enhance the lesson content. First, users could tap on the camera icons over geo-tagged photos in the "Geo-tagging" screen to show metadata information (See Figure 5.3, B). Second, users could interact with an activity map on the "A day in the life of Jane" screen to show possible consequences of photos sharing (See Figure 5.3, D). This interactive screen used a "trail" metaphor identified in our previous work [115] to convey the risks of leaving a digital trail on the Internet. Lastly, the comic concludes with a drag-and-drop mini quiz game that provides textual feedback to help users review the key concepts (See Figure 5.9). Detailed documentation of the user interaction is included in Appendix A.

5.3.2 Graphic Design

Each panel of the comic is carefully designed to create visually appealing compositions to capture readers' attention and interest. Basic graphic design principles [86] such as balance, movement, emphasis, repetition, proportion, and unity are applied to create a sense of harmony and cohesiveness to each comic panel. The main graphic design elements used in Secure Comics that lead readers through the layouts are the grid layout, points of focus, and directional flow.

Grid Layout: Secure Comics was designed with a 4 × 4 grid layout with white gutters (borders) and follows the traditional Western method of reading from left to

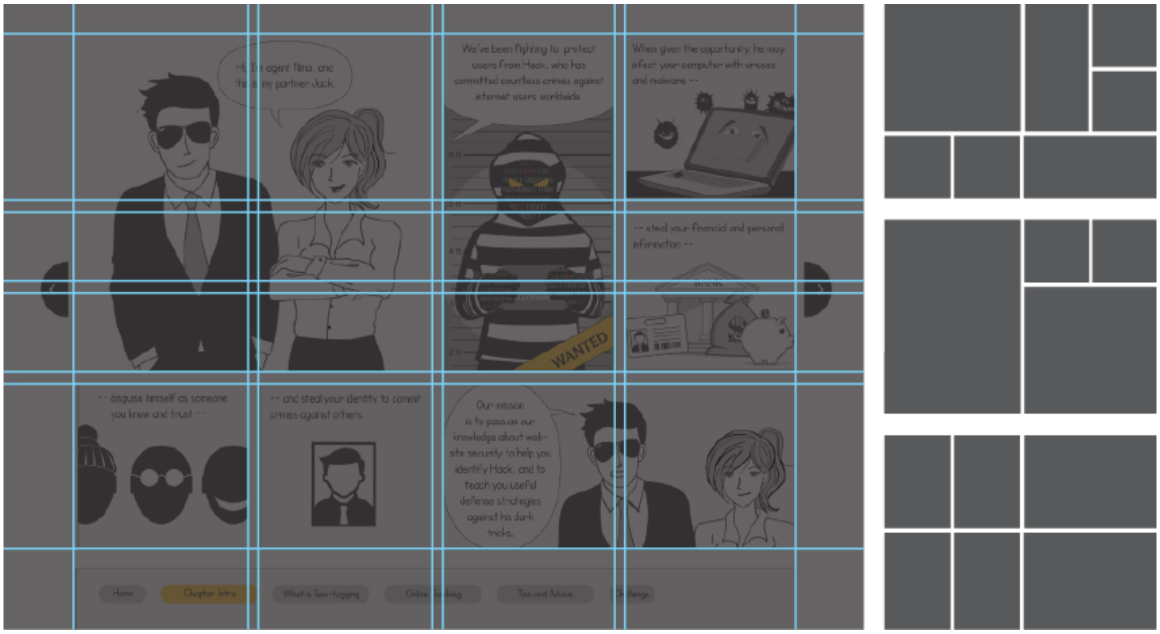

Hi, I'm agent Nina, and this is my partner Jack.
We've been fighting to protect users from Hack, who has committed countless crimes against internet users worldwide.
When given the opportunity, he may infect your computer with viruses and malware --
-- steal your financial and personal information --
BANK
WANTED
-- disguise himself as someone you know and trust --
-- and steal your identity to commit crimes against others.
Our misson is to pass on our knowledge about web-site security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.
Home
Chapter Intro
What is Geo-tagging
Online Tracking
Tips and Advice
Challenge

Figure 5.6: The grid layout system used in Secure Comic (left) and some of its possible configurations (right).

right and top down. Figure 5.6 shows the grid and a few of its many possible layout configurations. Squares and rectangles of the grid were sometimes split or merged to create interesting visual effects. This grid format was chosen because it offered a highly flexible compositional tool to arrange graphics and dialogue while conforming the artwork to a consistent visual style between the pages.

Points of focus: Once the grid system was established, we determined the location of the focal points for each panel. The centre of a panel typically created a strong focal point. For example, in Figure 5.7, we amplified the centre of focus with a graphic illustrated in a spiralling motion towards the centre to direct the readers' gaze to the character. Another technique we used was colouring points of interest. Since the beginning of the design, we made a conscious decision to use colour strategically rather than for decoration. In Secure Comics, colour is applied sparingly to highlight graphical elements to which we wanted to direct the readers' attention. Characters in Secure Comics usually face the reader and speak directly to them to capture their attention. In some cases, however, it was useful to manipulate the characters' gaze to direct readers' attention to the direction that the characters' is looking, as portrayed

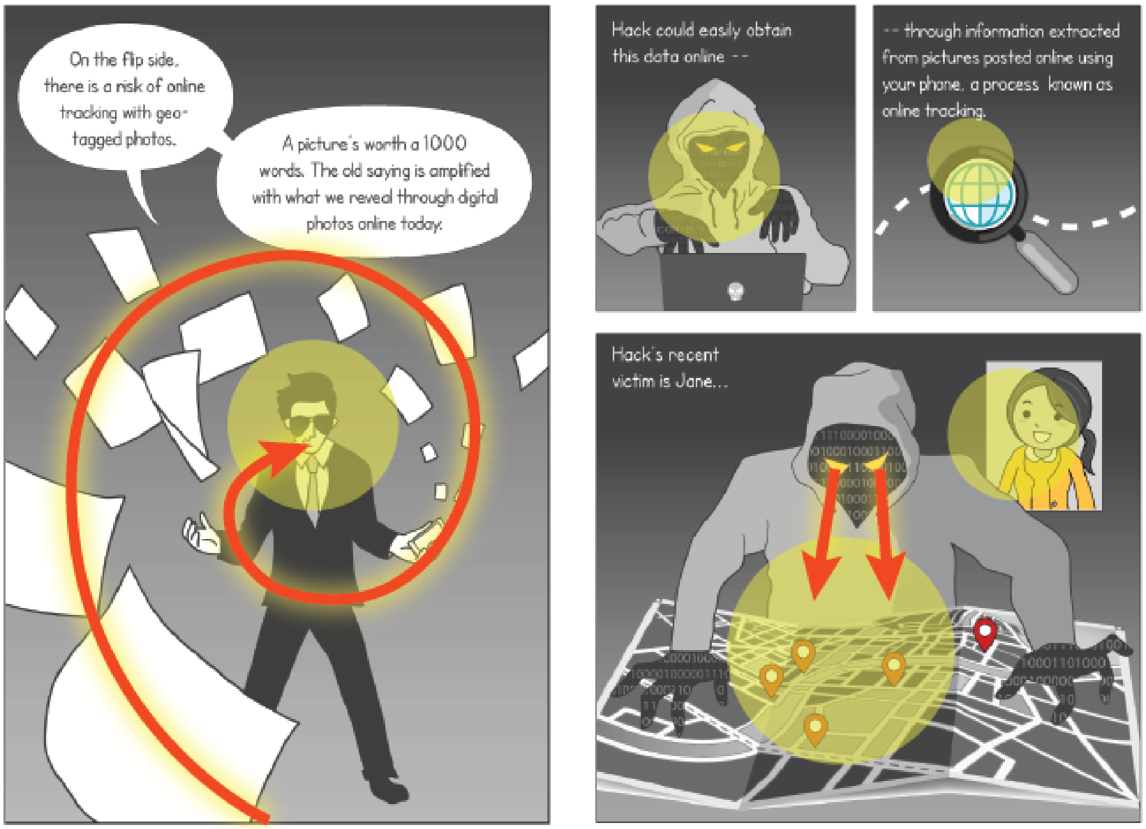

On the flip side, there is a risk of online tracking with geo-tagged photos.
A picture's worth a 1000 words. The old saying is amplified with what we reveal through digital photos online today.
Hack could easily obtain this data online --
-- through information extracted from pictures posted online using your phone, a process known as online tracking.
Hack's recent victim is Jane...

Figure 5.7: A panel of the comic highlighted with the placement of the focal points.

in Figure 5.7.

Directional flow: We worked with the composition and subtle graphical elements to direct readers to follow a certain reading path. For example, the meandering road in Figure 5.8 creates a subtle and subconscious flow on the page that prod reader to follow the character's story in a logical sequence. Readers' gaze move along this subtly implied line, using the road graphic, as well as the placement of the focal points, to guide them through the composition.

5.3.3 Navigation

Figure 5.9 shows Secure Comics' navigation as it appears on the iPad. The navigation is based on a page-by-page book metaphor. The application is set up to have pages, chapters, and bookmarks. To read the comic sequentially, users "turn" a page by tapping on a forward or backward button. Chapters can be selected from the main

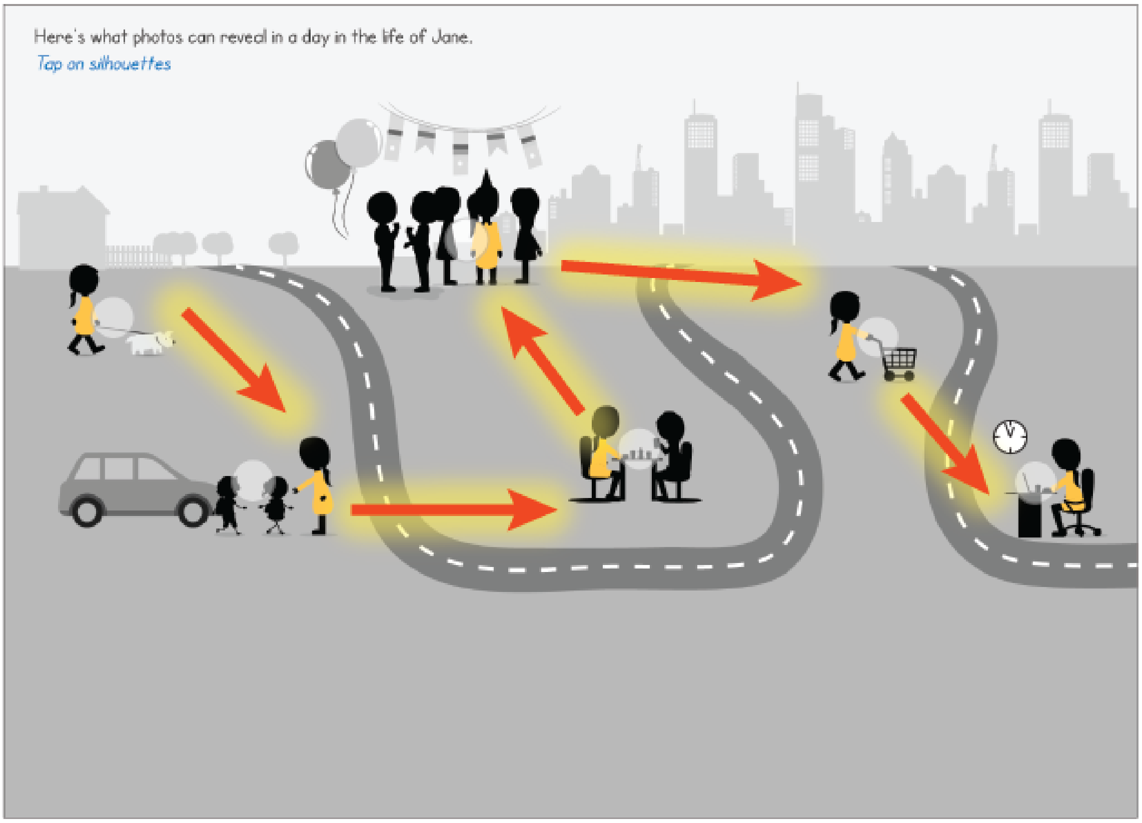
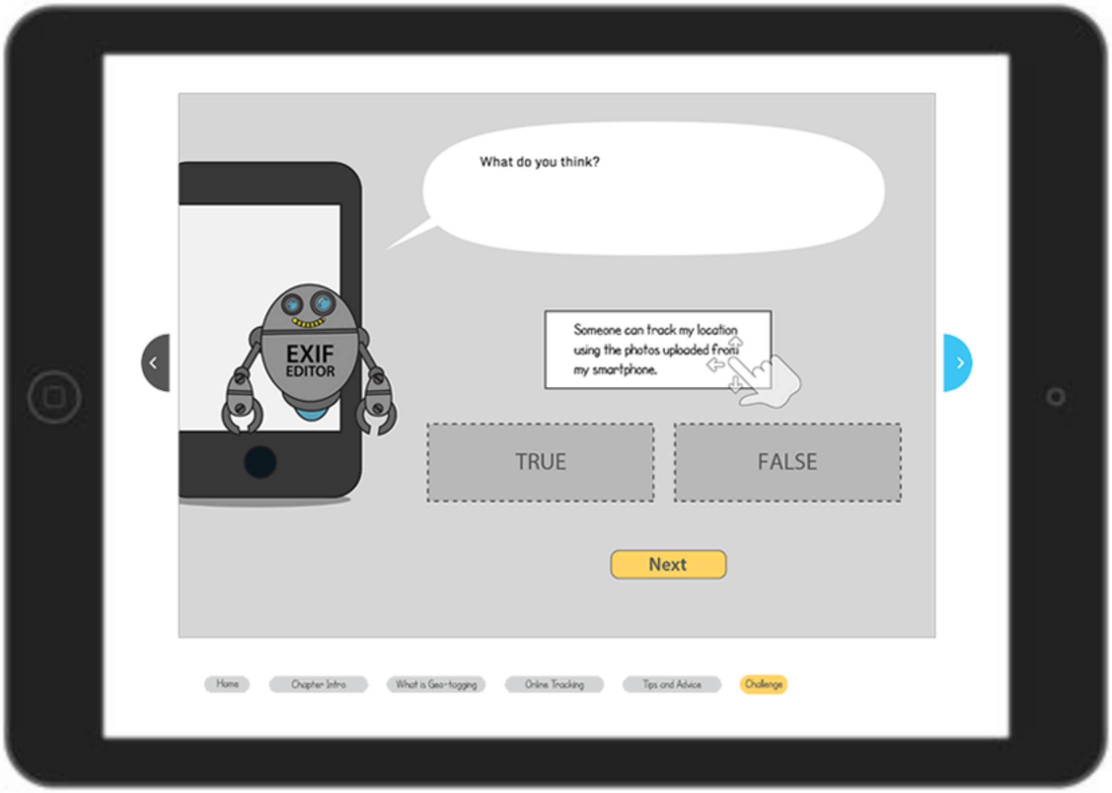


Figure 5.8: A panel of the comic highlighted with directional line of flow.

screen, and bookmarks that enable users to jump to a particular section in the comic can be selected from the bottom of the screen. Interactive features in the comic are highlighted by a pulsing circle symbol (e.g. Figure 5.3, D). and draggable objects are highlighted by a directional hand symbol (e.g. Figure 5.9).

5.4 Implementation Phase

The comics were drawn and produced by us using Adobe Creative Suite graphics software. We first created pencil sketches of the screens, then scanned and imported them into Adobe illustrator CS6. Using the sketches as a guide, we created original vector-based drawings using a Wacom Intuos Graphics Pen and Touch tablet. In some cases, we adapted stock images from Shutterstock for the backgrounds. The drawings were touched up in Adobe Photoshop CS6. Next, graphical assets were imported into a development application for implementation.



Someone can track my location using the photos uploaded from my smartphone.

Figure 5.9: The mini-quiz game from the privacy chapter of Secure Comics displayed on the iPad. Users navigate the comic screens by a forward and backward button. Bookmarks on the bottom of the screen enable users to jump to the beginning of a section in the comic.

Secure Comics was initially developed using Macromedia Flash as a web-based comic. When we started the first chapters of Secure Comics, Flash was a popular authoring tool commonly used for developing interactive web applications. Since Flash uses a timeline-based frame-by-frame development model and Actionscript scripting language, it was an appropriate choice as an authoring platform for a page-by-page interactive comic book. However, Macromedia Flash requires the Flash Player plug-in to be installed in web-browsers to run the application.

As we transitioned from working with adult users to children, we found this to be a major drawback as children often used tablets and smartphones that run on IOS devices with no Flash support. As an alternative, we migrated all Chapters of Secure Comics to GameSalad [64]for implementation. GameSalad is a mobile and web game development platform that allows developers to build, publish, and distribute self-publishing cross-platform games and interactive media. GameSalad was an attractive choice because it enabled rapid prototyping with a visual editor and an object behaviour logic system. The application provided a library of object behaviours such as movements, collisions, and attributes that can used to create rules and behaviour groups to create various animated or interaction effects quickly. We updated the graphics of Secure Comics for high-resolution retina displays and added background music to the title screen and sound effects to the comic screens. Secure Comics was re-released to the public as an app in the App Store[2], and as a HTML5 web comic[3].

5.5 Evaluation Phase 1: Adult Study

We first evaluated Secure Comics with 18 adult users to test the effectiveness of the comic and evaluated its perceived effectiveness, usefulness, and memorability. The study results helped to inform our user study with children. As a reference, we summarize the study with adults and the main results for the privacy chapter published in the International Journal of Human-Computer Interaction in 2016 [189].

Procedure: The study received approval from our University's Ethics Review Board. Participants were students and university staff recruited through an email mailing list. Participants were compensated $20 for their time. Each participant completed two one-on-one lab sessions. The first session was structured as follows:

- Participants completed a pre-test questionnaire assessing their current knowledge of smartphone geotagging and photo sharing behaviours.
- Participants viewed and interacted with the online comic. They were allowed as much time as needed to view the comic to learn about smartphone geotagging.
- Participants completed a questionnaire providing their perceptions and opinions of the prototype. The questionnaire included 5-point Likert scale questions, ranging from 1 (strongly disagree) to 5 (strongly agree). Some questions were

[2] https://itunes.apple.com/ca/app/secure-comics/id1130794100

[3] http://www.versipass.com/edusec/securecomics/app/app.html

reversed to avoid bias. The questionnaire also re-tested their knowledge of smartphone geotagging and photo sharing.

Fifteen participants returned approximately one week later to complete the second session. The session included a follow-up questionnaire and interview about the information they learned and their experience during the study.

Adults' Pre-Conceptualizations of Geo-tagging and Mobile Online Privacy: Adult users had a poor understanding of how geo-tagging works. Before viewing the comic, most participants thought geo-tagging is manually tagging a photo or a person to a location (i.e., checking-in friends on social media). They believed that others could only track explicitly shared location information. Alarmingly, only one participant specifically mentioned metadata containing geographical coordinates automatically attached to image files. Participants made their photo sharing decisions based on assumed privacy tolerance levels of others and the social context. Most were not very concerned about their online privacy because they believed that they had control over what they shared; they believed that they had nothing to hide; or they felt they were not vulnerable.

Comic's Effects on Adults' Privacy Behaviour and Understanding: One week after viewing the privacy comic, 53% of participants self-reported having changed location-based settings on their smartphones. These include disabling global positional systems (GPS) on their devices and removing location metadata from photos. Participants were also more aware of photo content that could reveal personal information. For example, one participant said, "Since viewing the material, I definitely took actions online and on my smartphone to protect my privacy online. I changed my settings on my phone. . . and I am also careful when uploading pictures in case there is anything in the background of the photo that could be used like my drivers' licence or a credit card." Another 27% of participants said that the comic has raised their awareness about online privacy and therefore motivated them to behave more cautiously online.

Participants showed excellent retention of knowledge one week after viewing the comic. We assessed retention based on our participants' ability to describe two major concepts conveyed in the comic, geo-tagging and EXIF (Exchangeable Image File).

All respondents were able to identify what geo-tagging means in the post-test compared to 53% in the pre-test. Similarly, 67% of respondents correctly described the EXIF concept compared to just 7% in the pre-test.

Perceived Effectiveness and Usefulness of the Comic: Adult evaluations for the *effectiveness* and *usefulness* of the privacy comic as an educational tool were highly positive. There was consensus among participants that presenting the information visually as a comic was easy to read and understand, and they reported a pleasurable learning experience. The comics took little time and effort to read but gave useful information about the threats and practical protection strategies. Participants believed presenting the information as a comic has positive effects on how well they could recall the advice later. After reading the comic, most participants believed they gained useful knowledge about topic, particularly for clarifying common misunderstandings and learning about preventive strategies. Our participants expressed interest in the narrative and the characters of Secure Comics and believed that the media would be suitable for a wide range of age groups, including children.

Motivated by the positive feedback we received from adult users and their recommendation for use of the comic with children, we conducted a second user study with children evaluating the Secure Comic on mobile online privacy. The study with children is reported in detail in Chapter 6.

Chapter 6

Secure Comics About Mobile Online Privacy: Evaluation

To explore the potential effectiveness of privacy and security educational tools at improving children's privacy knowledge and behaviour, we evaluated our work, Secure Comics, with children. Although the comic was initially created with a general audience in mind, the security content, format, and literacy level also seem appropriate for children 11 years and older.

This research extends our educational work with adult users [189], which showed that Secure Comics had positive effects on adults' understanding and management of their privacy and security. The work with children presented in this chapter has been accepted at the British HCI Conference, 2017.

6.1 Methodology

In our two-session between-subject study, the dependent variables are *privacy knowledge* and *privacy behaviour*, and the independent variable is the type of media (i.e., the comic or the same narrative text-only presentation). In our study, we used children's responses to situation-based scenarios as a proxy for real behaviour. The scenarios were created as realistically as possible with circumstances relevant to children. Furthermore, the questions were framed objectively with a clear context. In privacy and security research, measurements of real behaviour are often unethical and sometimes not possible without putting users in compromising situations. This issue is particularly sensitive when the participants are children. As an alternative, measurements of intent have been accepted as a reasonable proxy for behaviour in usable security literature [53].

The study is based on a between-subject pre-test, post-test, followup (PPF) design commonly used to study intervention effects in child and adolescent research [136]. In PPF design, the dependent variable is measured on three separate occasions to determine if an effect exists at the end of the intervention and persists beyond a specified period of time has passed after the end of the intervention [136]. The design is structured to measure the dependent variable first prior to intervention to establish a baseline, second at the end of the intervention, and third at a specified time period after the end of the intervention. In essence, the PPF design is an extension of the prepost design [136] to include two post-tests (i.e., post-test and followup). In our study, the followup is conducted after one week. One week interval is often used in recognition and recall based lab studies such as authentication (e.g., [32, 47]). The time frame was also reasonable for scheduling a followup for busy families.

Our study procedure is summarized in Table 6.1. In Session-I, the dependent variables were measured pre- (pre-test) and post-reading (post-test). In Session-II, the variables were measured a third time one week later (1-week-test). The tests were administered as interviews, which has many benefits over surveys for children 7 years and older, including reducing fatigue, increasing attention, and enabling children to clarify vague responses [152]. Our interviews with children were audio recorded and transcribed. Half of the child-parents pair were assigned to either the *comic* procedure or the *text* procedure (control).

Our research questions were: 1) Do the groups differ in privacy knowledge and behaviour from the pre-test to the post-test? 2) Do the groups differ in privacy knowledge and behaviour from the pre-test to the one-week-test? 3) Do the groups differ in privacy knowledge and behaviour from the post-test to the one-week-test?

6.1.1 Text Control

We selected text as the control condition because users typically read privacy and security information online through various types of textual communication such as privacy policies, warning dialogue boxes, and advice columns. The format also enabled us to convey the same educational content and narrative by isolating the textual content from the visuals, audio, and interactivity in the comic. Even though other methods are possible, they had limitations for our study. For example, it would be difficult to control for variability in a real-time lecture delivered by a teacher. Other time-bound media such as a filmed lecture or an instructional video reduces variability, but the content may need to be altered for adaptation to film. Furthermore, films are passively “watched”, whereas comics and text need to be actively “read”. Based on these considerations, text was the most appropriate control for our comic study.

The same-narrative text-only control condition was designed to read like a children’s storybook and replicated the same narrative flow as the comic. All textual information was retained from the comic. To compensate for the lack of visuals, we added scene descriptions and other descriptive textual information to create a comparable reading experience as the comic. For example, children who participated in the *comic* procedure read the screen shown in Figure 5.3, B, while children who participated in the *text* procedure read the following text segment:

> “Pictures taken by most smartphones automatically attach location based data called geo-tagging,” Jack continued. “Geo-tagging photos is a useful feature on the Internet, allowing people to share the location of experiences through their photos, such as where you took a picture of a sunset, an awesome event, or the location of that amazing restaurant you tried!”
>
> “On the flip side”, Jack cautioned, “there is a risk of online tracking with geo-tagged photos.” Jack pulls out a picture of dreamy beach sunset, a lively concert photo, and a picture of a delicious-looking plate of sushi. Upon closer inspection, the three photos displayed the following information:

IMG_3857.jpg Location: Cancún, Mexico Date: December 21, 2013 Time: 5:10pm Latitude: 21.1606 N Longitude: 86.8475 W	IMG_2457.jpg Location: Montreal, Canada Date: January 2, 2014 Time: 8:56pm Latitude: 45.5000 N Longitude: 73.5667 W	IMG_7584.jpg Location: Toronto, Canada Date: March 11, 2014 Time: 7:17pm Latitude: 43.7000 N Longitude: 79.4000 W

The *comic* group read Secure Comics on iPads; the *text* group read on 8.5” by 11” printouts. Screenshots of the comic are included in Appendix A. The text version is included in Appendix C.8.

Families were provided with 2 iPads or 2 printouts and chose to read together or independently for as long as they liked. Most child-parent pairs chose to read independently. Children took on average 10 minutes and 50 seconds to read the *comic* and 9 minutes and 40 seconds to read the *text*. Session-I took 40 minutes, and Session-II took 20 minutes overall.

6.1.2 Participants and Recruitment

Twenty-two children between the ages of 11 to 13 (10 male, 12 female, mean age = 11.9 yrs) participated in our REB approved study. Most were accompanied by mothers (one by a father). The parents were between the ages of 30 to 49 from a wide range of education and economic backgrounds, including a bachelor's degree (n = 13), college diploma (n = 3), high school diploma (n = 3), and graduate degrees (n = 3). Six mothers were stay-at-home moms; others worked in education (n = 6), social services (n = 1), business (n = 4), and healthcare (n = 5). All children regularly used a mobile device. Their main activities were Youtube (22/22), app-games (21), picture-taking (19), web-games (16), web browsing (16), messaging (16), music (15), and Netflix (15).

To recruit families, we posted announcements on local parenting groups on Facebook. The Facebook groups were public and anyone could post to share news, local events, and other types of information. Additionally, we contacted local education resources centers who forwarded our recruitment notice to parents on their email mailing lists. Parents signed informed consent forms, and the children gave verbal assent. Each family received a $20 honorarium. The participants were identified by codenames preserving the child-parent pair. For example, C1-comic is read as "child 1, comic condition", P2-text is read as "Parent 2, text condition", and C1-comic is the child of P1-comic. Child participants were pseudo-randomly assigned to either the *comic* (M = 5, F = 6, mean age = 12.1) or *text* condition (M = 5, F = 6, mean age = 11.6) but gender was balanced between conditions to avoid gender effects.

Procedure & Materials			
Ses.	**Participants**	**Comic Procedure**	**Text Procedure**
I	Parent	A) Demographic Questionnaires	A) Demographic Questionnaires
	Child	B) Pre-Test Interviews	B) Pre-Test Interviews
	Parent&Child	Read *comic*	Read *text*
	Parent	C) Adult Usability Questionnaire	N/A
	Child	C) Child Usability Questionnaire	
		B) Post-Test Interviews	B) Post-Test Interviews
1-week Interval			
II	Child	B) 1-Week-Test Interviews	B) 1-Week-Test Interviews
	Parent&Child	N/A	Read *comic*
	Parent		C) Adult Usability Questionnaire
	Child		C) Child Usability Questionnaire

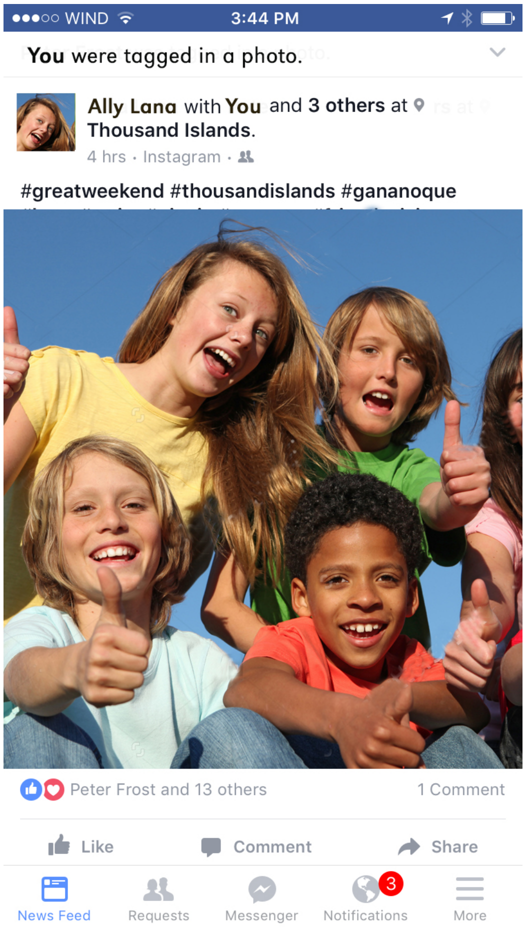
Table 6.1: Summary of the study procedure. The colours group similar activities together. Materials are described in Section 6.1.3

6.1.3 Evaluation Measures

In the following section, the evaluation measures are labelled according to the letter code listed in the study procedure in Table 6.1. All study material is included in Appendix C.

A) Demographic/Activities, Pre-Evaluation Questionnaires: All parents completed an Adult Demographic Questionnaire (age, gender, education, and occupation), and a Child Demographic (age, gender, grade) & Activities Questionnaire (children's daily device use duration and going online, types of devices, online activities. and whether children had prior privacy/safety education). The Pre-Evaluation Questionnaire for parents was intended to assess whether they have a dominant criteria for choosing educational apps for kids. Parents ranked the criteria "fun", "age-appropriateness", "ease of use", "educational value", and "effectiveness" from rank 1 (most important), to rank 5 (least important) .

B) Children's Privacy Tests: The tests included ten knowledge-based questions and four behaviour-based scenarios. To evaluate users' computer privacy and security intention and practices, we assess both knowledge and behavioural aspects. To measure *privacy knowledge*, children recalled information learned from the narrative (e.g., "what is online tracking?") and made inferences (e.g., "How does your smartphone



You were tagged in a photo.

Ally Lana with You and 3 others at Thousand Islands.

4 hrs · Instagram ·

#greatweekend #thousandislands #gananoque

Peter Frost and 13 others

1 Comment

Figure 6.1: An example of the supplementary visual aids used in the scenarios for both conditions.

track your location?"). To measure *privacy behaviour*, children responded to scenarios presented with visual aids. For example, children saw a screen capture of a social media post (see Figure 6.1) and read the following situation: "you took a group picture with your friends on a trip and one of them asked you to post the picture online, check-in your location, and tag everyone in it". Children explained what they would do and how the situation might affect their own and others' privacy. The pre-tests established a baseline for each child, and the questions were repeated verbatim in the post-tests. The 1-week-tests evaluated the same concepts but contained alternate scenarios.

C) Child & Parent Usability Questionnaire: All participants completed a usability evaluation of Secure Comics. We wanted to make the study experience fun for families by allowing the *text* group to also experience Secure Comics and complete a usability evaluation. The study procedure was designed to not confound other study measurements by having the *text* group view and evaluate Secure Comics only after they completed the privacy tests (see Table 6.1). To check for possible bias caused by the *text* group having previously read of the text-only format, we conducted Mann-Whitney U tests; they indicate that viewing order had no effects on children's opinions of the comic (Engagement: $U = 47.50, Z = -.97, p = .33$; Ease of Use: $U = 49.00, Z = -.84, p = .40$; Ease of Learning: $U = 55.00, Z = -.39, p = .70$). No significant differences were found between the conditions.

The child questionnaire contained eight questions. Engagement was measured using an Again-Again Table [139] asking: *1) Would you read the comic book again?* (coded 3 for "yes", 2 for "maybe" and 1 for "no"). The next five questions used the Smileyometer [139] (i.e., visual Likert-scales; 1 = least positive, 5 = most positive) to elicit opinions on the following: *2) How fun was the comic book? 3) How easy was it to use the comic book? 4) How well did you learn from the comic book? 5) How likeable were the characters? 6) How willing would you be to show the comic book to other kids?*. The last two are open-ended questions that asked: *7) What did you like about the comic book? 8) What did you dislike about the comic book?*. The parent version tested the same constructs using regular Likert-scales.

6.1.4 Interview Data Analysis

The transcribed interviews from audio recordings were organized in Excel into responses according to the interview questions. The primary researcher coded each of the participants' response (3 = very good, 2.5 = good, 2 = marginal, 1.5 = poor, 1 = very poor) in Excel for a total out of 30 for *privacy knowledge*, and 36 for *privacy behaviour*. A second undergraduate research assistant who helped to conduct the user study and transcription independently coded 50% of the responses. Prior to the analysis, the researchers read all of the transcriptions and discussed them together, and created an answer key outlining the target knowledge and behavioural criteria for the responses. For example, one scenario asks children to sign up for a social media account by entering personal information (the alternate scenario in the 1-week-test is to give personal information to receive a discount on an online store). The target behaviour is to press the “skip” button, or to enter non-identifiable information (e.g., a flower image as the profile picture). To receive a score of 3, children must meet the target behaviour and be able to explain why they should not give personal information. Those who met the target behaviour but were unable to explain why received a score of 2. If children did not know the answer or gave the wrong answer, they received a score of 1. Half scores were given for partially correct answers. A Cohen’s Kappa (k) test showed strong agreement between the two researchers’ analysis of the pre-test ($k = 0.9$, 95% CI: .8 to .9, $p < .001$), Post-test ($k = 0.8$, 95% CI: 0.7 to 0.9, $p < .001$), and 1-week-test ($k = 0.8$, 95% CI: 0.7 to 0.9, $p < .001$). In cases of disagreement, the two researchers discussed and consolidated the scores to be used in the final analysis.

6.2 Children’s Privacy Tests Results

We compared children’s knowledge and behaviour scores on three separate occasions during the study: pre-test, immediately after reading (post-test), and one week later. As recommended by Rausch et al. [136], we used one-way Analysis of Covariance (ANCOVA) tests to detect differences between groups in the post- and 1-week-tests using children’s pre-test scores as a covariate to control for their pre-existing knowledge and behaviour. Furthermore, we tested children’s 1-week privacy scores between the two conditions after controlling for their learned knowledge and behaviour using children’s post-test scores as a covariate. The results are summarized in Table 6.2 and visualized in Figure 6.2. The unadjusted and adjusted means used in the analysis are summarized in Table 6.3.

The assumptions for the ANCOVA were met: There was a linear relationship between the pre- and post-test, and the pre- and 1-week-test for each condition, as assessed by a visual inspection of scatterplots. There was homogeneity of regression slopes as there was no statistically significant interaction term between the covariate (i.e., pre-test) and the independent variables (i.e., *comic* and. *text*). We used the Shapiro-Wilk test to determine that the standardized residuals for the conditions and the overall model were normally distributed. A visual inspection of the standardized

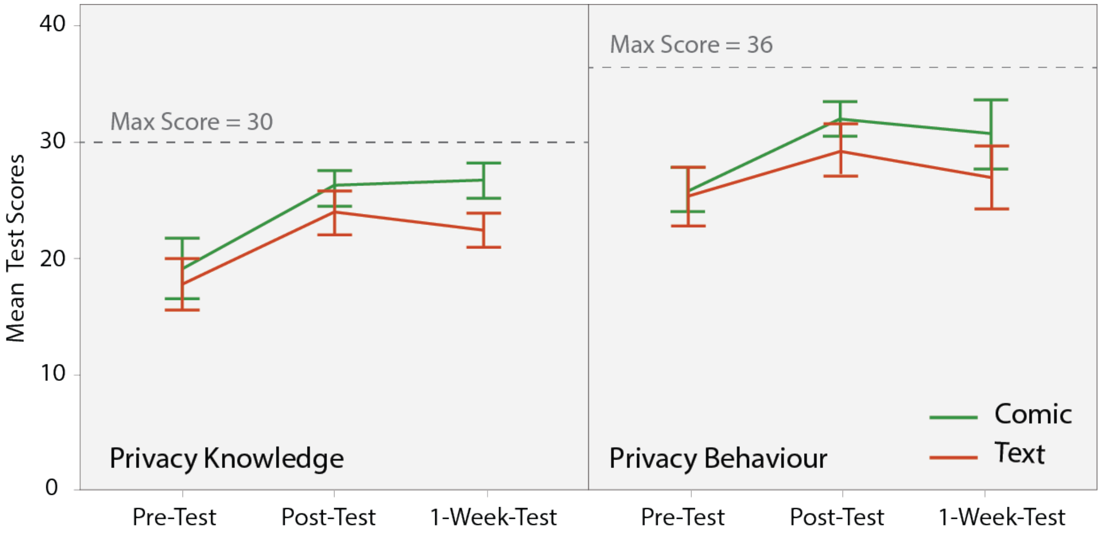


Figure 6.2: Summary of children's pre-, post-, and one-week-test scores between groups. Error Bars: 95% Confidence Interval (CI)

Privacy Knowledge			
Tests	*MD*	95% CI	*p*
Pre/Post	1.8	[-.3, 3.9]	.090
Pre/1-week	4.0	[2.0, 6.0]	**.001**
Post/1-week	3.1	[1.3, 5.0]	**.002**
Privacy Behaviour			
Pre/Post	2.2	[.5, 4.0]	**.013**
Pre/1-week	3.8	[.8, 7.0]	**.016**
Post/1-week	2.0	[-1.9, 6.0]	.304

Table 6.2: ANCOVA tests showing statistically significant differences between groups for *privacy knowledge* in the Pre/1-Week-Test and the Post/1-Week-Test. A statistically significant difference between groups for *privacy behaviour* was found in the Pre/Post-Test and the Pre/1-Week-Test. MD = Mean Difference, CI = Confidence Interval, p = Significance Level.

residuals plotted against the predicted values showed that there was homoscedasticity. One outlier in the knowledge post-test data of the *text* condition and one outlier in the 1-week-test behaviour data of the *comic* condition were replaced with the next lowest values in the group, as is standard practice.

Between-Subject Effects on Privacy Knowledge: Taking children's pre-existing knowledge (pre-test) into consideration by using the adjusted means of children's knowledge scores in Table 6.3, we found no statistically significant difference between

Privacy Knowledge						*Privacy Behaviour*			
		Unadjusted		Adjusted		Unadjusted		Adjusted	
Tests	Condition	M	SD	M	SE	M	SD	M	SE
Pre/Post	Comic	26.2	2.3	26.0	.7	14.5	2.6	14.1	.5
	Text	24.0	2.8	24.2	.7	13.5	2.7	13.9	.5
Pre/1-Week	Comic	26.8	2.3	26.6	.7	15.4	1.8	15.2	.4
	Text	22.5	2.2	22.6	.7	13.0	1.7	13.3	.4
Post/1-Week	Comic	26.8	2.3	26.2	.6	15.4	1.8	15.2	.4
	Text	22.5	2.2	23.0	.6	13.0	1.7	13.3	.4

Table 6.3: Adjusted and unadjusted means and variability for the Post-Test and 1-Week-Test privacy proficiency scores with Pre-Test privacy proficiency scores as a covariate, and 1-Week-Test privacy proficiency scores with Post-Test privacy proficiency scores as a covariate. Adjusted means are used in the analysis. M = Mean, SD = Standard Deviation, SE = Standard Error.

conditions for their post-test scores. Analysis of the 1-week-test scores however, showed a statistically significant difference between the conditions in privacy knowledge, $F(1, 19) = 18.5$, $p < .001$, partial $\eta^2 = .493$. 1-week privacy knowledge was greater in the *comic* group than in the *text* group. The post- vs. 1-week tests also showed a significant difference between groups, $F(1, 19) = 12.8$, $p = .002$, partial $\eta^2 = .403$. Specifically, the *comic* was significantly more successful than *text* at sustaining privacy knowledge after one week.

Between-Subject Effects on Privacy Behaviour: Using the adjusted means of children's behaviour scores in Table 6.3, we found a statistically significant difference between groups immediately after reading, $F(1, 19) = 7.5$, $p = .013$, partial $\eta^2 = .284$, and one week after reading $F(1, 19) = 7.0$, $p = .016$, partial $\eta^2 = .270$. The *comic* was more successful at influencing children's post-test and 1-week-test privacy behaviour than *text*.

6.2.1 Children's Privacy Tests Results Summary

Both the comic and text-only format improved children's privacy *knowledge* immediately after reading, but after one week, the *comic* group retained the learned knowledge while the *text* group forgot some of the knowledge. Children who read the comic were significantly more likely to choose privacy-preserving behaviours after reading

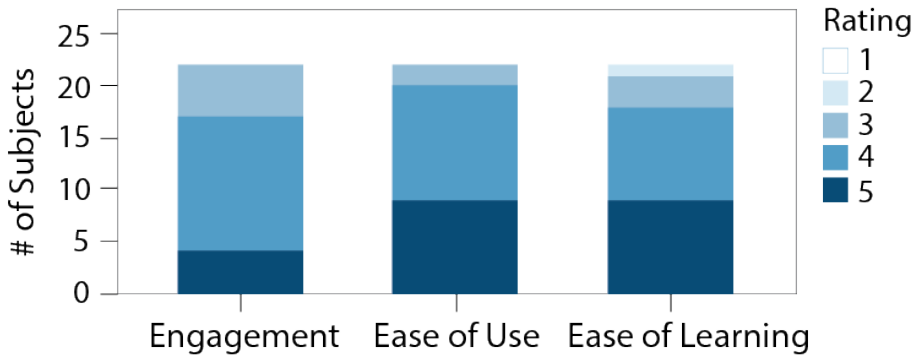


Figure 6.3: Summary of children's usability evaluations (5 = most positive).

and after one-week. Those in the *comic* condition showed greater increases in their privacy *knowledge* and *behaviour* scores, and maintained higher scores after one week, even when adjusted for variance in baseline *knowledge* and *behaviour*. The comic appears more effective than the text-only format at conveying knowledge and persuading children to consider privacy-preserving behaviours.

6.3 Usability of Secure Comics

Figure 6.3 shows children's opinions on engagement, ease of use, and ease of learning for the comic.

Secure Comics is engaging for children: Children's assessment of whether they would like to repeat the activity is highly correlated to engagement [139]. The Again-Again evaluations showed that more than half of children are confident that they would read Secure Comics again ("yes" $n = 13$, "maybe" $n = 9$, "no" $n = 0$). Furthermore, their Smileyometer evaluations showed a mean of 4/5 for "fun". Children said the learning experience was fun because of the graphical format and interactivity, and because the information is told through a story. C7-comic thought the comic was *"fun and interactive"*. C6-text thought the comic *"was funny"*. C1-text *"liked the graphic format and being able to interact with the comic"*. C3-comic *"liked the characters"*, and C2-text thought *"the drawings were cool"*. Children suggested less text and more character information, colour, and interactive challenges.

Secure Comics is easy to use for children: Children thought the interface was very ease to use (Mean = 4.3/5). The only difficulty we observed was the drag-and-drop quiz feature, where children preferred to tap. Some found certain "big words" difficult to understand like "geo-tagging".

Secure Comics made learning easy for children: Children felt they learned well (Mean = 4.2/5). C10-text said, *"a lot of people use electronics without caring. The comic helps people care more about their privacy."* C3-text felt *"there was a lot of information, but it was split up well."* C2-comic liked *"the different situations that could be relatable for people."*

Parents' feedback: Parents' pre-evaluation rankings of criteria in choosing an educational app for children 11 to 13 years old (1 = most important) showed that they had varying opinions. The rankings averaged at 2.5 for *educational value*, 2.6 for *effectiveness*, and 2.9 for *age-appropriateness.* It seemed that *fun* (mean = 3.4) and *ease of use* (mean = 3.6) were the least important criteria for parents.

Parents' post-evaluation of the comic (5 = most positive) was consistently positive across criteria, with 4.6 for *educational value*, 4.5 for *effectiveness*, 4.4 for *age-appropriateness*, 4.0 for *fun*, and 4.6 for *ease of use.* Parents felt that the comic *"used real-life situations, which facilitated discussion points and made the topic very relevant"*; *"The presentation is interactive and interesting, and it seemed less like "work" to review with [their] child"* (P3-text). Parents felt the comic format was very appropriate for kids: it *"helped [my child] learn more about privacy while doing this in a fun and gentle format"* (P4-comic); Another parent said, *"I liked that it explained a complicated and somewhat scary topic in a fun and easy to use way. I found 'A day in the life of Jane' very effective in showing how a hacker can track your movements throughout the day"* (P3-comic). To improve, parents suggested brighter colours, a deeper story, and more interactive features.

6.4 Discussion

In Chapter 3, we proposed a security behaviour model that described the likelihood of positive behaviour change if users have high security motivation and function mental models. Secure comics improved children's security motivation by providing insights into why it is necessary to follow secure practices. Furthermore, simplifying security content through graphical communication increased comprehension and supported children's conceptualizations of the risks.

6.4.1 Comics for Supporting Children's Memory

Our study found that both narrative formats supported children's short-term memory, but a visually rich comic was more successful than the text narrative at supporting knowledge retention. Working memory stores information in the short term, which can be retrieved to coordinate perception, long-term memory, and action [151]. Long-term memory retrieves information by consciously recalling previous experiences or known facts [151]. The comic narrative had superior immediate and 1-week effects on children's privacy knowledge and behaviour than the text narrative. After one week, the *comic* group maintained the learned knowledge while the *text* group forgot some of the knowledge learned during the first session.

The result supports Dual-Coding Theory that states the combination of related text and images increase long-term memory [34]. This result is also consistent with our previous study with adults [189], where participants showed an excellent retention of knowledge post-test and one week after viewing the comic. Another important source of motivation for learning is interest in the activity [175], such as learning while doing a fun recreational activity like playing video games. Video games motivate players to persevere through the game challenges and simultaneously teach players how to play because they incorporate good learning principles [67]. The relationships of learning and engagement is also explored in "Edutainment", which is educational media designed to both entertain and educate. The goal of edutainment is to "increase the audience's knowledge about an educational issue, create favourable attitudes, and change overt behaviour" [160]. However, researchers (e.g., [76]) caution that the overuse of multimedia in educational technology that do not support educational goals could distract learners from learning.

6.4.2 Comics for Persuading Privacy-Conscious Behaviour

We found the visually rich comic narrative is more effective at driving behaviour change than the text narrative. Children's response to situation-based scenarios dramatically improved after they read the comic. After one week, the *comic* group maintained privacy-conscious behaviour while the *text* group showed a decrease in desired behaviour. This suggests that the comic was more successful at sustaining changes in children's behaviour after one week. Positive behaviour change was also reported in our previous study with adults [189].

Several factors unique to children's behaviour were taken into consideration in this study. First, children are still developing new experiences with technology, and second, parents share the responsibility for managing their privacy and security. It is therefore impractical to expect certain behaviour from children, such as changing location-based settings on their smartphones because some may not own a personal smartphone (e.g., they borrow their parents') or they do not yet perform the activity that could put them at risk (e.g., they do not post pictures online because they are too young to have social media). These factors influence children's behaviour and could change over time as they age. Teaching appropriate behaviours and helping them become privacy-aware can help persuade them towards more independent privacy-conscious actions.

6.4.3 Challenges in Children's Privacy and Security Education

Privacy and security education has several unique challenges that could be addressed through comics. First, persuading children to behave in a privacy-preserving manner is difficult because, like adults, they typically do not regard privacy and security as primary concerns [182]. Children main use of mobile devices is for entertainment [166], and they may not be motivated to invest time to learn about privacy and security [80]. Our study showed that children found Secure Comics very engaging and fun to read. This suggests that embedding educational information in comics is a promising educational approach for children.

Second, security threats constantly change and evolve compared to other types of safety advice for children that is relatively unchanged over time, such as wearing a seatbelt. This makes it difficult to give children definitive protective advice. Privacy educational materials should therefore aim to teach critical-thinking and motivate children to consider the consequences of their online actions [166]. Privacy boundaries are also personal in nature. Users must choose how much they are willing to share for themselves. Educational material should, therefore, ensure that users understand potential consequences and tradeoffs of sharing information, rather than giving declarative rules that everyone must follow.

Furthermore, comics are an adaptable media where new content could be created more quickly and at relatively low cost compared to other media types such as films, animation, or games. New educational content could be added as a part of a series and present the story within the context of an overarching narrative. Secure Comics presently has three chapters, each addressing one topic through the story. The chapter on mobile online privacy is the third installment in the series. Several families expressed interest reading the other chapters on passwords and malware after completing the study.

Third, users rely on mental models[1] to make privacy and security decisions. Children have poor mental models of privacy that are even less developed than adults' [191] and this could have negative consequences on their protection behaviour. Secure comics use narrative storytelling, simple textual explanations, and graphics to illustrate complex privacy and security concepts. Children who read Secure Comics demonstrated careful, logical, and conscious thinking about different scenarios in the post- and 1-week-tests and acted in a more privacy-preserving manner on both occasions compared to the control condition. This suggests that comics helped children to develop richer mental models than textual information, which had positive influences on their privacy behaviour.

6.4.4 Future Improvements

Our study suggests that visual narratives such as comics increased children's interest and engagement in learning about privacy and security. However, since Secure Comics was initially designed for adults, several improvements could be made for children.

[1] A *mental model* is a simplified internal concept of how something works in the real world [39].

Narrative and character depth: Children liked the characters in Secure Comics, but wanted more in-depth character development and a richer narrative. Several children commented that they would like to learn more about Jack, Nina, and Hack. We believe this is partially because children in our study saw only one chapter of the three-part comic series. Other chapters built on the narrative to include other privacy and security stories and include additional character development.

However, we believe improvements could be made to the narrative structure. Even though the narrative in Secure Comics is based on a series of events, it does not follow a traditional 5-part plot structure (i.e., exposition, conflict, rising action, climax, falling action, and resolution [61]). We believe that a tailored narrative with a traditional plot structure to dramatize events and characters that are similar to children of our age group would increase the appeal of the narrative.

Colour: Secure Comics was designed in traditional black and white comic style. Colour was used sparingly as a signalling device to the elements of interest. However, feedback from children suggested they preferred more colourful visual styles. This was unsurprising as research shows that children are attracted to bright colours [33] because they stand out more in their field of vision [17]. In our future work, colour would be an important design element for children.

Interactive Features: Children liked the interactive features in Secure Comics and requested additional features to be included. Feedback from parents also suggests that a higher level of interactivity would be more engaging for children.

Text: Secure Comics included moderate amount of text but required some effort to read. Although we did not observe children skipping content or having difficulties reading, "too many words" was one of the things that children disliked about the comic. Feedback suggested that the amount of information was a lot for children to take in, and they had some difficulties with technical words like "geo-tagging". Furthermore, a larger font size is preferred by children. Simplifying the content and reducing amount of text would be an even more important design consideration for younger children.

6.4.5 Limitations

Our scenario-based lab assessments of children's behaviour are used as a proxy for real life behaviour due to ethical concerns of putting children in compromising online situations. Although a promising approach, children's responses to scenarios may not directly translate to real life behaviour. Our 1-week study provided some indication of the long-term educational effects, and could be extended in a future longitudinal study. The effects of the comic could also be compared to other media types and teaching formats in a future study. Our results may only be applicable for children 11 years and older due to younger children's developing working and long-term memory capabilities [44]. However, we hypothesize that tailored educational narrative about online privacy created especially for children would have even more persuasive effects.

6.5 Conclusion

This chapter reported on the effectiveness of an educational comic about mobile online privacy at influencing children's privacy knowledge and behaviour. Using a between-subject study design (*comic* vs. same-narrative *text*) with 22 child-parent pairs, we found that both narrative types showed statically significant improvements in privacy *knowledge* immediately after reading, but the *comic* was more effective than *text* for retaining knowledge after one week. Furthermore, the comic was persuasive in changing children's reported privacy *behaviour*. Children and parents found the comic easy to learn for children, engaging, and easy to use, showing that it is an appropriate educational format for children. Since Secure Comics were initially designed for a general audience, we believe narratives tailored to children with characters that are similar to them could further increase the persuasive appeal, as it is explored in Chapter 8 and 9. As an intermediary step, Chapter 7 discusses a study to gain an understanding of online privacy from children's perspective in order to design effective educational software for them.

Chapter 7

Children's Privacy Models

7.1 Children and Parents' Perception of Mobile Threats

To design better privacy and security technologies for children, we studied the factors relating to privacy, security, and threats surrounding the use of mobile media by Canadian children aged 7 to 11 years. To fully understand children's perception of these topics, it is critical to include parents' perspective, particularly because parents play an active role in children's daily interaction with mobile devices and they share the responsibility for managing children's privacy and security [2]. The study consists of a qualitative comparative analysis of children and parents' perception of the threats and the protection strategies employed by these families. The work presented in this chapter has been published at the 2016 ACM SIGCHI Interaction Design and Children (IDC) Conference [191].

The study explores three related research questions: R1) *Children's privacy*: How do children conceptualize privacy and what does 'being private' mean for children? R2) *Perceptions of potential threats*: How do children and parents' perceptions of threats surrounding mobile media differ from each other? R3) *Strategies to protect children*: How do parents protect their children from the perceived threats surrounding mobile media?

We draw from more than 35 hours of transcribed audio interviews with 14 families. Using qualitative content analysis [54], we identified four models of online privacy held by children. Our analysis suggest that the younger children's understanding of online privacy is 'to be alone' or 'to hide secrets or special things,' whereas older children had a more refined understanding. Furthermore, we identified four child-adversary threat models (*child-peers, child-media, child-strangers, and child-parents*) from the children and five child-adversary threat models (*child-peers, child-media, child-strangers, child-technology, and child-self*) from the parents. We found large discrepancies in threat perceptions between the two groups. Children showed a very preliminary understanding of the harm caused, and perceived internal threats from siblings and parents to be more imminent than external threats from friends, strangers or online media. Parents on the other hand, were more worried about external threats, and used a variety of protection strategies to minimize children's exposure to them.

7.2 Methodology

7.2.1 Ethics and Recruitment

Our methodology was reviewed by the Carleton University Research Ethics Board-B. The participants were recruited through invitations shared with local community Facebook groups and mailing lists for children's educational resource centres who forwarded our recruitment notice to parents. The participants are from the cities of Ottawa, Kitchener-Waterloo, and Cambridge in the province of Ontario, Canada. Participation was limited to children aged seven to eleven, and one child per family who used at least one mobile device on a regular basis. The adult participants were the parents or legal guardians of the child participants. The interviews typically took place at a public location of the parents' choice, such as at a community centre or a library. We obtained written consent from the adult participant followed by verbal informed assent from the child. Each parent and child was awarded a $10 gift card (a $20 honorarium per family).

7.2.2 Participants and Procedure

We audio-recorded semi-structured interviews with 14 parent-child dyads. The children were between the ages of seven to eleven; eight were male ($Mean$ age = 8.75) and six were female ($Mean$ age = 8). Nine adult were between the ages of 31 and 40, five were between the ages of 41 and 50, and one was between the ages of 21 and 30. Eleven mothers and three fathers volunteered to accompany their child to the study. Four mothers were stay-at-home moms and the other parents had full time jobs in a variety of professions. Nine had a Bachelor's degree, four had a college diploma, one had a Masters degree, and another had a high school diploma.

All of the families had two or more children living in the household. The majority of children (12/14, 86%) lived with two parents, while two children lived with a single mother. They all had Internet access at home and were regular users of mobile devices.

The parent-child dyads were briefed about the study together but interviewed separately. The adult participant completed a basic demographic questionnaire on gender, age, level of education, and occupation. A semi-structured interview followed with the adult participant, then with the child participant.

The interview questions were targeted to gain insight into children's use of mobile devices and their understanding of privacy related risks from two perspectives: from the point of view of the parent and from the perspective of the child. During the child interview, the parent was encouraged to be nearby but not sitting directly with the child to give the child more freedom to speak. However, we accommodated families who wished to sit together. If the child voluntarily disclosed sensitive personal information during the interview, it was removed from the transcription. Participants were not required to use any devices during the interview but some children voluntarily brought their devices to the study. At the end of each interview, the participants were debriefed and awarded their honorarium. Each dyad session took around one hour, approximately evenly split between the adult and child.

7.2.3 Qualitative Data Analysis

We applied qualitative content analysis methodology from Elo & Kyngäs [54] to analyze the data. Content analysis is a research method for making valid inferences from data and their context, with the purpose of providing knowledge, new insights, and a representation of facts [93]. The research method may be used to analyze either qualitative or quantitative data, and be applied in an inductive or deductive way, as determined by the purpose of the study [54]. According to Elo & Kyngäs, the aim of content analysis is "to attain a condensed and broad description of the phenomenon, and the outcome of the analysis is concepts or categories describing the phenomenon."

The qualitative content analysis process is illustrated in Figure 7.1. The beginning of the process is similar to thematic analysis [19], where the researcher gains a

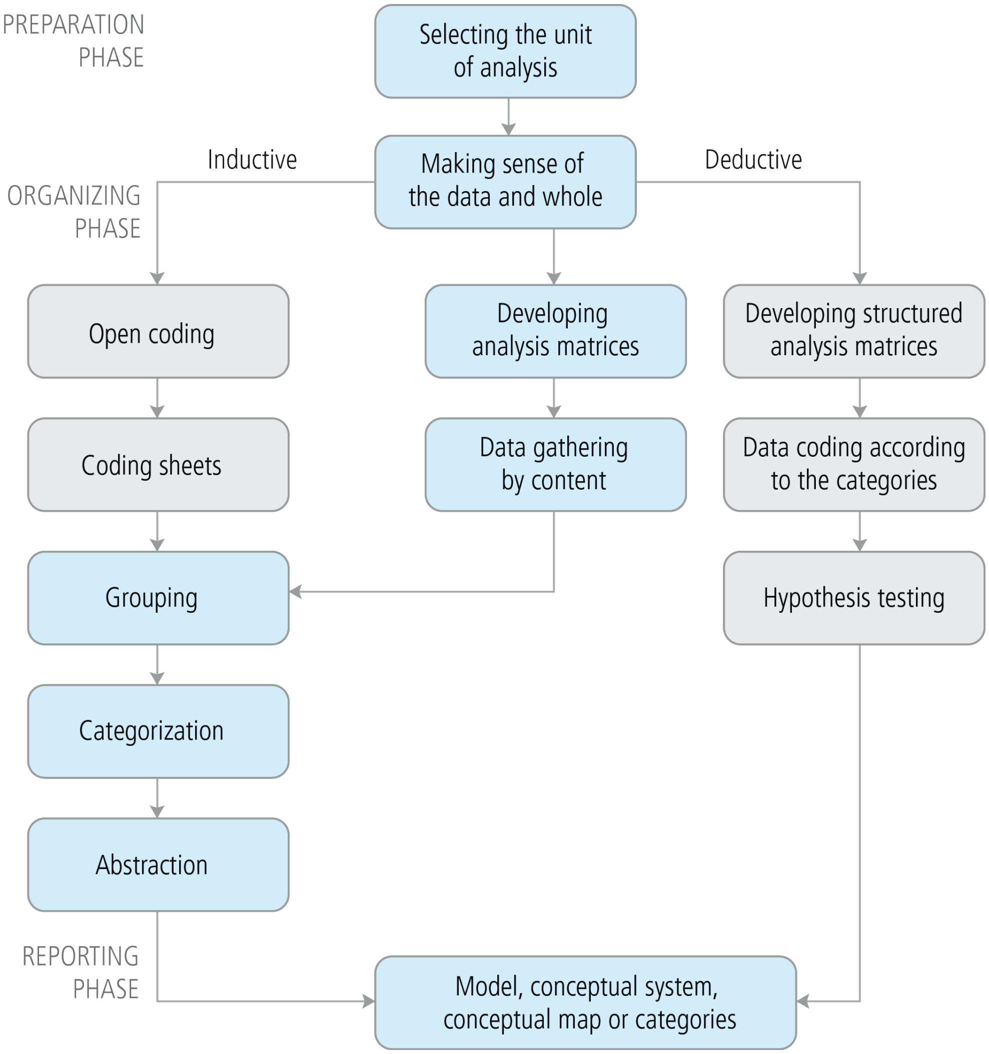

PREPARATION PHASE
Selecting the unit of analysis
Inductive
Making sense of the data and whole
Deductive
ORGANIZING PHASE
Open coding
Developing analysis matrices
Developing structured analysis matrices
Coding sheets
Data gathering by content
Data coding according to the categories
Grouping
Hypothesis testing
Categorization
Abstraction
REPORTING PHASE
Model, conceptual system, conceptual map or categories

Figure 7.1: Preparation, organizing, and reporting phases in the qualitative content analysis process. The process we used in our study is highlighted in blue. The graphic is adapted and redrawn from the original by Elo & Kyngäs [54].

sense of the whole dataset by reading the data transcripts several times, a process called *preparation* in content analysis. Next, the researcher chooses whether to use an inductive or deductive approach. Our analysis used the deductive approach, where interview responses are organized along four main themes: general device use, children's activities on the device, maintenance of the device, and children's online privacy knowledge. We began the analysis by organizing the responses into their themes and subthemes listed in Table 7.1. These were developed based on our research questions

THEME	SUBTHEME
General Device Use	How are the mobile devices used Where are the mobile devices used What children have on mobile devices
Activities	What activities are performed Who do children communicate with
Device Maintenance	Who is responsible for device maintenance Who can install apps/games on the mobile device
Online Privacy	What do children know about online privacy What does privacy mean to children What do children do to stay safe online Who teaches children about online privacy How do children behave online How do children manage passwords When do children talk to strangers online What information should/should not be shared

Table 7.1: Interview responses were organized into themes and subthemes at the beginning of the analysis process.

and prior research surveys conducted with children by Common Sense Media [143] and MediaSmarts [163].

In next step of the deductive approach, a structured or unconstrained categorization matrix of analysis can be used [54]. Since the purpose of our study is to find new insights within the context of the themes/subthemes, we used an unconstrained matrix to create categories within the bounds of our research questions. For example, for the threats perceived by parents to harm children, we identified a matrix of 8 categories and organized and summarized the responses accordingly. An example of the analysis is provided in Table 7.2

In content analysis, groupings of categories and sub-categories are further refined through *abstraction*. We identified relationships between the categories and sub-categories and integrated the results to form children's privacy models and child-parent threat models. Figure 7.2 shows an example of the abstraction process.

The primary researcher exhaustively coded all interview transcripts and conducted analysis to identify themes relevant to our research questions. To increase the reliability of the analysis, a graduate research assistant performed additional analysis for 20 percent of the transcripts (i.e., transcripts for three children and three parents)

What are the threats perceived by parents that harm children?	
Category	**Response Description**
Inappropriate content	Parental control is set for YouTube. Parents monitor what apps children have on their devices daily. Mom deletes violent or frightening games immediately.
Inappropriate apps	Kid's apps account is linked through mom's email.
Social media	Mom worries about kids over sharing information.
Device addiction	Kids go on the devices too often; parents try to limit the hours when they can. Parents "don't get" the value of certain activities like feeding a virtual character.
Falling behind technology	Mom worries that she is not proficient enough to use technology that kids use to properly monitor them and keep them from harm.
Stranger-danger	Mom worries about kids talking to strangers online whose true identity is unknown.
Older siblings	Device is shared among younger and older siblings in the same household. Older sibling installs app that is not age-appropriate for her little brother.
Friends	Mom has no control over what her kids have access to at their friends' house.

Table 7.2: A portion of the threats and responses in the categorization matrix for the threats that could harm children as perceived by parents.

based on the theme of perceived threats using codes that emerged from the original analysis identified by the primary researcher. For example, the primary researcher identified 51 excerpts from the three child-parent pairs concerning threats perceived by children and threats perceived by parents that harm children, and created 13 codes that describe them. The primary researcher provided the research assistant with the code list, an Excel spread sheet containing the itemized excerpts, and the original transcripts with the excerpts shown in context of the interview. Independently, the research assistant first read the original transcripts several times to gain an overall understanding, then applied codes from the code list to the excepts from the three children and three parents in Excel. After coding was complete, the two researchers met and discussed the results. In cases of disagreement, the researchers either resolved the disagreement by reaching a common understanding, or retained the differences in the analysis. In the latter case, we used codes applied by both researchers. For

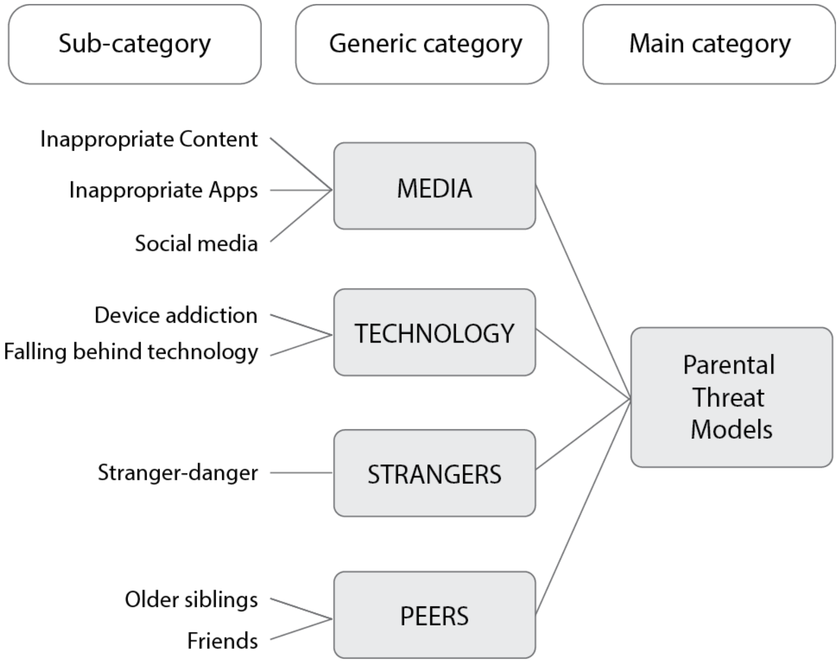


Figure 7.2: An example of the abstraction process of the threats that could harm children as perceived by parents.

example, in a disagreement where one researcher applied code #1 and the other researcher applied code #6 to an excerpt, both codes were counted in the groupings of categories and sub-categories during the analysis process. A Cohen's Kappa (k) test showed that there was strong agreement between the two researchers' analysis, $k = 0.93$ (95% CI, 0.86 to 1.00), $p < 0.005$.

To protect the participants' identities, we will refer to each child by a pseudonym, followed by their age and gender (e.g., Ella, 8f). The adult participants will be addressed directly as the child's parent (e.g., Ella's mother). Their pseudonyms and demographics are summarized in Table 7.3.

7.3 Interview Results

To provide context for subsequent sections on Children's Privacy Models (Section 7.3.2), Children's Threat Models (Section 7.3.3), and Parental Threat Models and Protection (Section 7.3.4), we begin with our findings on children's general device use, account management, and password management to understand the roles that children and adults play in the usage of mobile devices within the home environment.

7.3.1 Children's Interaction with Mobile Devices

Children's screen-time activities

Our results showed that children engaged in limited types of online activities and had very small online social circles. They used mobile devices primarily for entertainment and were consumers rather than creators of online content.

Playing games and watching YouTube trumped all other activities on mobile devices. All of the children regularly used the devices for gaming. Some popular games mentioned include Minecraft, Tettoria, Clash of Clans, and Dragon City. Most children (12/14) also watched YouTube videos. They were attracted to "funny" and "hilarious" content, Minecraft clips, game tutorials, and episodes from popular kids TV shows. None of the children posted online content or wrote comments. About half of the children watched Kids' Netflix (6/14) and used a search engine (7/14) primarily for school related work. Texting/messaging (4/14) and email (4/14) were less common and restricted to family, teachers, or friends that the child knew offline. Other less frequent activities reported were listening to music (2/14) and using the device's camera to take pictures (3/14). Only two children had social media – one had a Facebook account that is used for playing games, not for posting or commenting; the other had an Instagram account for sharing pictures with family members. In both cases, parents set up the accounts with the highest privacy settings, and only close family members could view or comment.

P. #	**Pseudonym**	**Age**	**Gender**	**P. #**	**Pseudonym**	**Age**	**Gender**
1.	Ella	8	F	**8.**	Tyler	10	M
2.	Alex	7	M	**9.**	Luke	11	M
3.	Jake	11	M	**10.**	Adam	9	M
4.	Mary	9	F	**11.**	Anna	8	F
5.	Kyle	7	M	**12.**	Maya	7	F
6.	Ryan	7	M	**13.**	Lily	8	F
7.	Ava	9	F	**14.**	Dave	8	M

Table 7.3: Child participants organized by their participant number, pseudonym, age, and gender.

Device sharing

The most popular device used among children were tablets (10/14), followed by iPod Touch (3/14), and handheld gaming systems (1/14). Children preferred tablets due to the large screen size. All households owned secondary devices that the children occasionally used, including other tablets, iPods, iPhones and Android phones, but none owned a mobile phone for the children's personal use.

Common among all families in the study was that one or more devices in the household were shared at least occasionally between siblings or with the parents. Parents shared their smartphones with their children primarily for convenience since they restrict children from taking their own devices outside of the house for fear of loss or damage. Parents often lent their smartphones to children to keep them entertained. In households with more than one child, devices were often shared between siblings.

Account management

In all families interviewed, parents were responsible for the management of children's online accounts. The types of accounts that children used were for downloading apps (e.g., App Store, Google Play Store), email, online gaming, and social media. Children's online accounts were always created and managed with an adult's help. Parents always had full access and knew the passwords for monitoring account activities and account recovery in case the child forgets the password.

For services requiring credit card information (e.g., App Store), children used their parent's account with permission. Half required explicit consent from the parents to download apps. Parents either entered the password directly on the device, or managed a linked account where app download requests were forwarded to the parents' phone. The other half was allowed to download free apps on their own, but the children must receive permission prior to download. Additionally, parents periodically screened the mobile device to weed out "bad" apps and many used parental control tools. In both groups, parents made the ultimate download decision and had the final say in whether an app can be kept or deleted.

Many children (9/14) owned email accounts that they did not use. The parents explained that the emails were created on occasions when the child needed it to sign up for another account. Adam's mother said that her son *"wanted to play the Facebook game,"* and *"he needed an email to get a Facebook account"*; Maya's mother created an email account so her daughter could get iTunes; Anna's mother created the account to sign her daughter up for a game. Parents also set up emails for future use. For convenience, Anna's mother set up email accounts for all of her kids when the eldest started school, even though the younger siblings did not yet need them. Ryan's father prepared an email account for his son as an upcoming "birthday gift".

Password management

The burden of remembering passwords for children's accounts usually fell on adults (parents and teachers). In the largest family we interviewed, all five children had individual email accounts and passwords managed by the mother (Adam's mother). Children frequently forgot their passwords, so they were encouraged by parents and teachers to create easy to remember dictionary passwords (e.g., "apple"). Adults always had a copy of the account information. If the account was created for school, the teacher provided parents with the login information. Not surprisingly, many adults used coping strategies like writing passwords down. To highlight the challenges and risks, we give Mary's mother's story of an incident at school:

> *The teacher had passwords written down because apparently, [the email accounts] are setup with the school board and if the kids were to lose their passwords, they have to call somebody at the school board, which could take some time, which means the kid wouldn't be able to get into the account. So, the teacher had written all the passwords down and hid it in her desk. I think one of the students saw, copied some, and then hacked in.*

All of the children had a basic understanding that passwords are secrets, but very few could explain why passwords should not be shared. Some examples from our interviews are: Kyle (7m) thinks that passwords should not be shared simply because *"no one wants you to know what it is!"* His parents do not share their passwords with him, and therefore he should not share his passwords with others. Ava (9f) might share her password with a friend that she trusts. Tyler (10m) revealed his iPad unlock

PIN to his friends *"because they are not going remember it."* Alex (7m) could not explain why sharing is risky but stated that he *"just [don't] feel like it sharing it."* One parent (Jake's father) suggested, *"It's intuitive not to share it,"* because *"they'll know my passwords are secret before they get their own passwords."*

Children had a very vague definition of who constituted a stranger. For example, Ryan (7m) believed that it is acceptable to share passwords with somebody he already knows like his best friend. Strangers approved by parents were considered safe, such as the researchers who interviewed them. One child (Maya, 7f) blurted out her password that her mother made for her during the interview. Contradictory to her behaviour, the child also said that she would not share her passwords with her mother (even though the parent made the password), brother, or strangers.

7.3.2 Children's Privacy Models

Livingstone [98] suggests that definitions for the concept of privacy are either centred on keeping information out of the public domain or centred on determining (or controlling, or knowing) which personal information is available to whom. Half of the children interviewed showed a lack of understanding about what it means to be private online. From their explanations, we identified four privacy models. Children with the first two models resorted to traditional definitions of physical privacy like "to be alone", or " hide secrets or special things". Children with the remaining two models had a preliminary understanding of online privacy that is based on notions of safety like "to keep things to yourself" and "to not talk to strangers".

Privacy is to be Alone

This group accounted for 36% (5/14). Privacy is analogous to "being alone" or "to be by myself". Several of the descriptions involved physically confining oneself to a room such as *"if you need to go somewhere and you want it to be private, you shut the door and you really lock it"* (Mary, 9f); *"When you are taking a shower, and no one's coming in. You are in the room by yourself"* (Tyler, 10m). One child described instances when he should leave other people alone because they are doing something "bad" on the computer, and *"[others] should just leave them alone"* (Dave, 8m).

Privacy is to Hide Secrets or Special Things

Three children believed that being private is *"when you hide something... something that's very special"* (Maya, 7f). Maya referred to hiding a physical item like her iPad, because *"you could have a little brother and they could break something."* Other children referred to hiding a secret that *"you don't want anyone to know"* (Kyle, 7m), and that you should *"not tell people what you have like stuff that you are not supposed to tell other people, like passwords"* (Ella, 8f). However, this was the only secret thing that Ella could identify.

Privacy is to Keep Things to Yourself

Four children had a basic understanding that online privacy is *"keeping your things and events in your life to yourself"* (Luke, 11m); things like *"your own personal data, which people can take and you want to keep them private for only yourself"* (Adam, 9m). Jake (11m) also believed that he should not give away anything about himself that is too personal. Ava (9f) cautioned that you should not *"post anything you don't want to post. If you post it, you might regret it later"*. All four children with this model are in the older age group (ages 9-11).

Privacy is to Not Talk to Strangers

Two children believed that *"privacy means you don't go lurking around people that you don't know, like you don't go play a game with a teenager that wants to know who I am and where I live. It's about keeping it safe"* (Ryan, 7m). Anna (8f) believed that being private means you should avoid the risks of someone *"being rude to you"* online. Both descriptions of privacy were framed as safety concerns.

7.3.3 Children's Threat Models

Children showed concerns for four child-adversary threat models: child-peers, child-parent, child-stranger, and child-media. Children had little protection strategies of their own. Their response to a threat is usually evasive or reactionary, such as avoiding content with "bad" words or becoming "upset" when something bad happens.

Child-Peers

Most children (12/14) considered siblings, friends, and other kids to be a threat they face on a day-to-day basis.

Siblings: The children in our study lived in homes with at least one other sibling. Adam (9m) for example, shared his device with four other siblings. Children constantly fought over screen-time on shared devices. Dave (8m) explained, *"I don't like (my brother) there because he always touches the iPad when I'm trying to watch a video."* Siblings could also damage children's special things so they need to be protected. Maya (7f) complained that her little brother *"always tries to blow up [her] stuff"* on Minecraft. Other risks of sharing a secret with siblings were that they are *"bad at keeping secrets"* (Luke, 11m).

Friends: Children also protected themselves from their friends. For example, when asked about whether they shared passwords with friends, Tyler (10m) said "no", because *"they could send something to somebody, like say a bad word, and [he] could get in trouble."* Ava (9f) would not trust her best friend with her password because *"she's done things"* before. For game accounts, children's main concern was that others could "mess up" their game if they had access. Ryan (7m) explained, *"it might be a little dangerous [to share my password], because they would be able to play as me and do things that you know, like mess up my game. They can sell cars or they'll just spend all my money in the game, and then I'll have completely no money and then I can't upgrade my powers or anything."*

Child-Media

Nine children identified media as a potential threat but had a vague understanding of the harm.

"Bad" Media: Swearing, violence, and adult content were described as "bad". Kyle (7m) said he would not watch violent stuff online, only "funny stuff". Mary (9f) was aware that she was not allowed to get any apps with guns or watch videos with violence. Dave (8m) did not think he had any "bad" games because he was not allowed to download a gun game that he wanted. He watched YouTube videos from a "safe" channel that did not contain swear words. Anna (8f) thought there are "bad"

words on Facebook. When inquired about why those things were “bad”, most of the children could not explain. Alex (7m) knew that he was not allowed to watch violent videos, but was confused about why he was allowed to *“watch stuff with swords but not guns”*. Most of the children had a very abstract understanding of these concepts and appeared to be following the rules set by the adults out of respect.

Child-Strangers

Most children believed that you should not talk to strangers offline. Ryan (7m) said, *“stranger-danger I learn almost everywhere I go.”* However, we found that only 33% (5/14) of children viewed it as an online threat.

“Mean” Strangers: Strangers are typically judged by their friendliness online. The perceived harm from strangers is often viewed as trivial, such as being teased. Anna (8f) thought that you might want to hide things from a stranger, such as your real name so people could not make fun of your funny middle name. Jake (11m) believed that it was acceptable to show other kids pictures of yourself but maybe not older people, because *“younger kids are not allowed to do certain things but older kids are.”* One child (Alex, 7m) felt that giving personal information to strangers have no direct impact on himself, but might cause dangers to others. For example, he said that he would not tell a stranger where he goes to school because *“they might not be nice and they are going to rob the school.”* Only two children (Ryan, 7m, and Kyle, 7m) we interviewed perceived it as a real threat:

> *You don’t know if he’s actually friendly or just hanging friendly. Then when you meet him in real life, he wants to hurt you or something. You don’t go lurking around people that you don’t know, like you don’t go playing a game with a teenager that wants to know who I am and where I live. It’s about keeping it safe.* (Ryan, 7m)

Kyle (7m) said that staying safe online means not contacting anybody who is “not nice” because they might try to bully him. Most of the other children’s perception of the harm caused by strangers suggests that they do not see stranger-danger as an imminent or serious threat online.

Child-Parents

Four children saw parents as a risk to their privacy and special things, but were generally obedient to the rules and punishment imposed by parents.

"Protective" Parents: They respected their parents' wishes even though they did not always understand why. For example Tyler (10m) said, *"I'm usually not allowed chatting with people, like people playing a game, but I feel like you're allowed to talk to them... but I don't. My mom doesn't want me to do it."* Maya (7f) expressed annoyance that her parents delete her apps. Adam (9m) cleared his browsing history to evade monitoring. Several of the parents took away the children's device as punishment when they misbehaved and this was sometimes viewed as a threat.

7.3.4 Parental Threat Models and Protection Strategies

Parents identified five types of child/adversary threat models: child-media, child-technology, child-stranger, child-peers and child-self. To protect children against the threats, we found that parents employed a set of protection strategies, summarized in Table 7.4.

Child-Media

Children's exposure to inappropriate online media is one of the top concerns. Most parents interviewed (13/14) expressed worries about the content/media that children could access on their mobile device. We identified three sub-categories of such threats. For each of the sub-categories, we first describe the threat from the parents' perspective, and then describe the protective measures practiced.

Inappropriate Content: The "inappropriate content" described by parents pertains to sexual and violent content, cruelty, coarse language, and other types of adult content. All of the parents expressed explicit concerns about children accessing inappropriate content even though only two parents had actually experienced a real incident with their children. Alex (7m) was caught watching a YouTube video that contained guns and violence, and Ella (8f) was found watching a video that contained sexual content at a friend's house.

Parents *Restrict-Access* to inappropriate videos, and demand the children to *Unplug-as-Punishment* if they misbehaved. Dave's mother thought that although children are generally aware of what parents consider "bad", they get confused if it is an adult cartoon (e.g., South Park). Parents *Set-Parental-Control* for YouTube, Netflix, and browsers. They regularly *Check-Browsing-History* and *Monitor* what children search and download on their devices. If violent or frightening games were found, parents would *Delete-Apps* immediately. Many parents screen the apps before children can download them. Parents used a variety of ways to *Screen-Prior-to-Download*. They judged the appropriateness of the apps based on how they looked, app description, reviews, and age rating, but the information was not always reliable. Kyle's parent described an incident when they thought an app contained a bad word:

> *The small thumbnail picture [of the app] had the word "flick" on it... but the "l" and the "i" are mixed together and I thought it was an "U", and so then I said that it had a really bad F-word on it and that he wasn't allowed to play that game because I didn't want games with that word. So, one of his friends said, "I have that game, there are no bad words", and then he said something about you have to "flick" things away, and I said "oh, it says flick. Oh!" And then we understood.*

A few other parents read app recommendations from parenting magazines. Mary's parent admitted that sometimes choosing apps is a matter of "trial and error", but parents could always *Delete-Apps* later.

All of the children *Ask-for-Permission* to download an app, even though half could download free apps on their own. Half of the parents *Restrict-Access* to password protected accounts for purchases, such as the App Store or iTunes.

App Permissions: A few parents worried about what apps could access to on the mobile devices, such as the camera, photos, microphone, location, and personal information. Tyler's parent shared an internet hoax she learned about the app "My Talking Angela" (a chatterbot app) that rumoured to encourage children to disclose personal information using the game's text-chat feature, which was then exploited by pedophiles. The story highlighted fears from parents about what apps could access on their children's devices.

Surprisingly, very few parents from this group actually read app permissions during downloads. We found that parents used a "trial and error" method to periodically *Check-App-Permissions* in game settings after the apps were downloaded, and *Delete-Apps* if they felt they accessed too much information. For example, Mary's parent described her reaction to a game called Clumsy Ninja that had hidden features:

> *Sometimes it's a trial and error where [my daughter] gets something and then all of a sudden I will see, like there's a ninja one that she has, that you can take pictures on. I saw it, deleted it, read about it, she got it again. . . the pictures go to our pictures file. So sometimes, it's trial and error where I didn't realize that it had any picture or video options.*

Some parents reported difficulties in managing app settings. *"It's pretty complicated"*, said Adam's parent, *"it seems like every company is making it more complicated for people to access their privacy settings, and it's frustrating."*

Social Media: Our findings from Section 7.3.1 suggest that children aged seven to eleven have minimal interactions with social media. Only two children used a social media account and they did very little with it. Parents *Check-Privacy-Settings* and *Screen-Contacts* to ensure that only family and close friends can contact the child. Only 4 parents (29%) were worried about social media since most children did not have access. Parents explained that the children *"are too young"* and that *"[social media] is unnecessary"* for their age (Maya's parent). The parent elaborated further, *"I mean, what are they going to do on there? There's a lot of things that come up on there that is inappropriate. You know what I mean? Even for myself my privacy settings are so high. So yeah I think she's too young. I don't see her using that for quite a while."* Most of the parents believed that the appropriate age for social media is around 11 or 12 years old. *"We haven't said 'no' to Facebook,"* Anna's parent clarified, *"but right now the answer is no. She has asked a couple of times, but no you are eight! I know what comes across my feed! I think a lot of people put too much of their business on there I think that's dangerous."*

Parents expressed their resolve to *Prohibit-Use-Until-Older* for *"as long as they can"* (Anna's parent). These parents said that if their children were to get social media, they would demand *Access-to-the-Account* and closely *Monitor* its use.

Protection Strategies	Description	M: Inappropriate Content	M: App Permissions	M: Social Media	T: Device Addiction	T: Falling Behind Tech.	ST: Strangers	P: Older Siblings	P: Friends	S: Self
Monitor	Parent oversees device interaction.	♦		♦			♦	♦	♦	♦
Access-to-the-Account	Parent has full access to the account.			♦					♦	♦
Link-the-Accounts	Child's account is linked to the parent's account.							♦	♦	
Ask-for-Permission	Child asks for permission before use.	♦								
Prohibit-Use-Until-Older	Access is prohibited until the child is older.			♦			♦			
Restrict-Access	The child does not have access.	♦				♦			♦	♦
Limit-Screen-Time	The child's time on the device is limited by the parent.				♦					♦
Delete-Apps	Parent removes apps from the device.	♦	♦							
Screen-Prior-to-Download	Parent approves or denies app downloads.	♦								
Screen-Contacts	Parent approves or denies whom the child can contact.			♦			♦		♦	
Check-Browsing-History	Parent checks child's browsing history.	♦								
Set-Parental-Control	Parent uses parental control tools.	♦						♦		
Check-Privacy-Settings	Parent sets privacy settings.			♦			♦			
Check-App-Permissions	Parent checks what apps have access to on the device.		♦							
Educate-About-the-Threats	Parent speaks to the child about the threat.				♦		♦			
Unplug-as-Punishment	Parent denies access to the device if the child misbehaves.	♦								
Update-Tech-Knowledge	Parent keeps technology knowledge up-to-date.		♦			♦				
Use-Safe-Texting	Child can only send predefined messages.						♦			

Table 7.4: Summary of protection strategies used by parents to protect children against each perceived threat. M = Media, T = Technology, ST = Strangers, P = Peers, S = Self, ♦ = Parent uses the protection strategy.

Child-Technology

Six parents (43%) worried about the impact of technology on children. We identified two sub-categories this threat. The first category describes parents' effort to limit the use of technology for the fear of device addiction. The second category describes parents' anxieties to keep up with technology to properly protect their children.

Device Addiction: Most parents limited the duration of device use from 20 minutes to one hour on weekdays and longer on weekends. Many parents voiced concerns about children spending too much time on their mobile devices. If parents did not *Limit-Screen-Time*, kids will *"go on it all day if they can"* (Maya's parent). Parents also *Educate-About-the-Threats*; Mary's parent elaborated: *"We had a talk about addiction. We explained that addiction could be to the technology, to games... If I would allow it, she would be on her iPad for like 8 hours straight. She would even skip meals. She's very stimulated by the colours, movements, music, and sound on the iPad." "She's very smart,"* the parent continued, *"she can see that we are preoccupied with her sister or supper, and she would say, 'I have to go to the washroom,' and she'll go and try to sneak in a video..."*

Despite the effort, parents found it *"hard to get away from screen time, because there's so much movies that are online that you want to watch. There's so much learning material for children, but it's so convenient that it became an inconvenience"* (Adam's parent). Parents wanted more human-to-human interaction with their children. One parent also expressed frustration that she did not understand the value of certain game activities like feeding a virtual pet on time (Maya's parent).

Falling Behind Technology: Parents who were not technologically savvy expressed fear of falling behind the technology used by children. Dave's mother felt that keeping up with technology and knowing what kids are into is the only way to properly monitor them. Ava's mother was also troubled by the fact that kids *"know a lot more [than her]"*, and described how she spent three hours with a consultant when she purchased a mobile device for her daughter to learn about the settings, parental controls, and other functionalities of the device. *"This is what my daughter is going to be doing with it,"* she said, *"I want to be able to monitor it."* Parents either *Update-Tech-Knowledge* or *Restrict-Access* to unfamiliar technology. Ava's mother admitted, *"I* *limit technology because I'm not very savvy with it and I don't want her to be getting into things that are too far over my head that I can't monitor."*

Child-Strangers

Threats from strangers, dubbed "stranger-danger" by the parents, were identified by the majority (13/14) as a major concern, even though none of the children had an incident with a stranger online. Parents worried about children over-sharing information about themselves and talking to strangers whose true identity is unknown. Maya's mother commented,

> *There are certain people on YouTube who play (Minecraft) and [my daughter] wants to meet them and I'm like no, that's not going to happen. I've talked to her about privacy, about what's appropriate and what's not appropriate, what you should or should not be giving out.*

Most parents agreed that children have the basic knowledge to not talk to strangers offline because they learned about "stranger-danger" and "bullying" concepts from a very young age. For example, Ryan (7m) learned about these concepts from a karate teacher. However, there's a disconnect for them between online and offline dangers. *"I worry about that,"* said Anna's mother, *"especially my son. He's the friendliest kid you'll ever meet. He loves to talk and he loves to be everybody's friend, so that worries me. He knows in person not to talk to strangers, but of course online is totally different."* Adam's parent also believed that kids have the basic knowledge about safety like not giving out phone numbers, but are naïve about other things. Maya's mother worried that kids would *"not know things like you think you are talking to Donna and it's really Joe that's 45."* Similarly, Kyle's parent said that the thought of enabling children to contact other people made her nervous. Alex's mother also did not allow her son to chat online because *"you never know who's on the other side."*

Most children had online access only to people with whom they also had offline contact. Parents *Screen-Contacts* so that children could only send text messages to family and close friends. For example, Kyle's parent said,

> *He's got very few addresses in there. So it's only the people that we know*

> *and approve of that he can text, like his uncle or his stepbrothers. Sometimes he'll take funny pictures of toys that they are playing with and send those. Or sometimes if he is with his dad and he's built something cool out of Lego or something, he'll take a picture and text that to me.*

Parents generally *Prohibit-Use-Until-Older* of online chat and text messaging apps. They *Monitor* who they talk to, and *Educate-About-the-Threats* such as talking to strangers online. They gave advice such as *"avoid answering questions unless you know exactly who the person is, like your friend across the street"* (Jake's parent). For the few children with social media, parents *Screen-Contacts* and *Check-Privacy-Settings* to ensure that they cannot be contacted by strangers. Some parents *Use-Safe-Texting* apps so that the child could select from a set of predefined messages. For example, Tyler (10m) could send generic messages like 'good luck' to communicate with other players in an online game. Mary (9f) used a safe-texting app connected to a doll where she could send text messages and chat with the doll.

Child-Peers

Some parents (8/14) believed that online dangers could be caused by another child, usually the child's friends and older siblings.

Older Siblings: Older siblings could expose inappropriate content to younger siblings. Parents found it difficult to *Set-Parental-Control* when there are multiple children living in the household. Ella's mother explained,

> *What [my older daughter] is aware of and knows is very different from what Ella is aware of and knows. [my older daughter] already had sex education and she's in grade 5. She's aware of that and Ella isn't. As a parent, I would like to maintain that innocence, so the games should just be fun, interactive, and age appropriate. Some of the older games are very age inappropriate, you know, big boobs... that's for teenagers.*

Parents did not have good strategies for protecting children from older siblings other than to *Monitor* them. Some parents *Link-the-Accounts* between siblings for easier monitoring.

Friends: Parents felt that children's friends have a huge influence. Most parents said they trusted their own children, but were wary of their friends. Ava's mother explained, *"she's very responsible. Sometimes the kids themselves are not mischievous but it's their friends that are instigators. They don't understand the influence that others have on them."* Ella's mother described an incident when her daughter slept at a friend's house and they decided to check out a porn site. Parents worried about losing control of what the child is exposed to outside of their own homes. Adam's mother said, when they *"go to their friend's house, I can't control what they get from their friends."* Lily's parent worried about social influence, peer pressure, and the type of friends they talk to.

Parents have *Access-to-the-Account* and regularly *Monitor* account activities. Tyler's mother goes through the child's text messages secretly at night when he is asleep. Parents *Screen-Contacts* on mobile devices and on social media. Some parents *Link-the-Accounts* to their own device so they can *Monitor* activities. When a certain friend is over for a visit, Ava's parent *Restrict-Access* to devices to reduce chances of getting into mischief. Parents *Screen-Prior-to-Download* any games recommended by a friend.

Child-Self

Half of the parents believed that children are young and naïve and therefore should be protected from potential harm caused by their own actions. A common attitude among the parents was that *"kids will be kids. They are curious and want to try things"* (Ella's mother). Children are sheltered by parents from any potential external harm. Jake's father explained:

> *Right now they are kind of at the innocent stage of using iPads or technology where they have been shown how to do something... how to specifically do a few things and not much else... I don't even think he has really gone on the Internet on the iPad before. It's really through applications and that's it. My daughter is the same way. They are very limited in their understanding and knowledge of what these things can do.*

Child's Threat Models	Ella	Alex	Jake	Mary	Kyle	Ryan	Ava	Tyler	Luke	Adam	Anna	Maya	Lily	Dave	Total
Child-peers	★	★				★	★	★	★	★	★	★	★	★	11
Child-media		★	★	★	★	★	★		★		★			★	9
Child-stranger		★	★		★	★						★			5
Child-parents				★				★		★		★			4
Parent's Threat Models															
Child-peers	♦				♦		♦	♦		♦	♦	♦	♦	♦	9
Child-media	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	13
Child-stranger	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦		12
Child-technology				♦			♦			♦	♦	♦	♦		6
Child-self	♦		♦			♦				♦	♦	♦		♦	7

Table 7.5: Comparative summary of the threat models we identified in parent-child dyads. ★ = Child has the model. ♦ = Parent has the model.

Children were either deliberately not exposed to certain technology, or they were restricted from accessing certain tools or services. Ryan (7m) explained that his father would not give him his Apple Store password because *"he thinks I'd buy any random game. All the games!"*, but Ryan explained that he is actually quite selective of the games he likes. He was also curious about sharing pictures on mom's Facebook page, but was told that he is not old enough for the activity. Children were therefore limited in their usage of some technology and from partaking in certain social activities.

Parents *Monitor* children to protect them against self-inflicted harm. If the child has an online account, parents usually have full *Access-to-the-account.* They would *Prohibit-Use-Until-Older* of certain tools and services. To prevent children from spending too much time on mobile devices; parents *Limit-Screen-Time.*

7.4 Interview Results Summary

We summarize the findings based on the three research questions we set out to answer.

R1) Children's privacy: Children's understanding of external threats is very basic and reflects their experiences with offline safety. Therefore, the majority of the children's privacy models consist of "to be alone" or "to hide secrets or special things". Others showed rudimentary understanding that privacy means "to keep things to yourself", or "to not talk to strangers".

R2) Perceptions of potential threats: We identified four threat models perceived by children aged 7 to 11 and five threat models perceived by their parents, summarized in Table 7.5. Our results show large discrepancies of perceived threats within the child-parent dyads. Most children (11/14) thought friends and siblings posed a threat because they could tamper with their device, compete for screen-time, "mess up" their game, or do things on the device that could get them into trouble with adults. Dangers coming from media (9/11) were mainly exposure to bad words, violence, and other adult content, but the real harm perceived by children seemed to be the punishment from adults for viewing "bad" content. Threats from strangers were brought up by a small number of children (5/14), but the risks perceived were limited to getting teased or bullied. Parents on the other hand, perceived more severe external risks from peers (9/14), media (13/14), and strangers (12/14). Additionally, they identified threats from technology (6/14), and from the children themselves (7/14).

R3) Strategies to protect children: Parents protect children against potential threats by exercising a variety of protection strategies (See Table 7.4). Our findings from *R2* suggest that a relationship exists between the perceived threats and the protection strategies used; most protection strategies are intended to protect children from external threats.

Children and parents' perceptions of threat models help to explain how they prevent internal and external threats. Parents employed protection strategies to protect children mainly from perceived external threats that may or may not pose real dangers to children; they were often exercised at the cost of invading children's privacy. Children's threat models were conceived based on their perception of physical privacy. There were major differences between children's and adult's threat models that could influence their privacy-preserving behaviour.

7.5 Discussion

Consistent with literature on children's use of mobile devices [99, 143, 166], we found that children's primary activities are playing games and watching videos. Younger children do not manage their own accounts or passwords. They have small online social circles, which consisted of family, extended family, and close friends only.

As it might be expected, there is a clear gap between threats perceived by children and adults. Children showed less concern for online dangers because they do not yet know how to apply the concept of privacy online. The protection strategies practiced by the parents suggest that the lack of apprehension is largely due to the fact that young children are strongly sheltered by parents from having an online presence. Our findings show that parents perceived external threats (i.e., media, strangers, peers-friends, technology) to be more prevalent than internal threats (i.e., self, peers-siblings). In reality, we found that privacy and security risks from an internal family member or a friend are far more common than harm caused by cybercriminals or outsiders. For example, even though the majority of parents (13/14) believed strangers to pose a serious threat to children, none had experienced an incident where a stranger contacted a child online. It is difficult to determine however, whether parents' protective measures directly resulted in the reduction of external risks encountered by their children. Even so, our findings suggest that it is much more likely that children experience invasions of privacy and security from other members of the household, from friends, and from teachers. Children are constantly put under adult surveillance and do not have rights to privacy on their own accounts. Causes for breaches of privacy and security often came from a trusted adult. Several incidences came up in our interviews, including one described in Section 7.3.1 where a teacher wrote down all of the children's passwords and they got stolen by a student. Children were encouraged by adults to choose weak, easy-to-remember passwords, which could be quickly cracked in a dictionary password guessing attack. Most children owned unused password-protected accounts that were created by an adult. Although few children had an online presence on social media, parents frequently posted pictures of children on Facebook. Conversely, parents also faced risks from children. All parents interviewed shared at least one online account with their children, usually for making app purchases. Half of the children had access to the account (although they said they would still ask for permission first). They either knew the password, or had the password autosaved. Children could potentially misuse the account and credit card information. If they misbehaved under the account name, it could have a negative impact on the adult's credibility. Some security threats from children identified by the parents were password guessing, shoulder surfing, unauthorized access to device or apps, disclosure of parents' information to others, and losing the device with the account information.

Parents were conflicted between wanting to teach kids about online dangers for safety, but also wanting to shelter them from online negativity. Luke's mother explained, *"I wouldn't want to teach them about all the negative things that can happen... and I try not to go into detail about everything that's out there... they'll never sleep again."* Parents cautioned that children should not be exposed to privacy/security education too young. Parents feel that a lot of educational material is more suitable for older kids. Mary's mother described a presentation about online privacy at her child's school: *"The material is over their heads, like talking about Twitter and Facebook, which [the kids] are not really aware of."* Younger children need something that is relevant for their own age. We suggest that education about online privacy and security for young children should work with their existing privacy models to gently introduce them to the concepts. The four privacy models and four threat models from this paper could serve as a starting point.

7.5.1 Limitations

In our study, we cannot estimate how prevalent the models we identified are in children and adults due to our sample size. Our data also may not exhaustively cover all of the models existing in the population. We do, however, contribute to the understanding of young children's interactions with mobile media by putting forth a variety of children's privacy models and identified existing differences in the threat models perceived by children and their parents.

7.6 Conclusion

The rise in mobile media use by children has heightened parents' concerns for their online safety. Through semi-structured interviews of parent-child dyads, we explore the perceived privacy and security threats faced by children aged seven to eleven along with the protection mechanisms employed. We identified four models of privacy held by children. Furthermore, we found that children's concerns fit into four child-adversary threat models: *child-peers, child-media, child-strangers, and child-parents.* Their concerns differed from the five threat models held by the parents: *child-peers, child-media, child-strangers, child-technology, and child-self.* Parents used a variety of protection strategies to minimize children's exposure to external threats. In reality, however, our results suggest that privacy and security risks from an internal family member or a friend are far more common than harm from outsiders.

This work suggests that children have different privacy and security needs than adults. Young children have underdeveloped models of privacy, and their threat models mainly consist of internal threats from family members. Ironically, our results suggest that the threats perceived by children are actually closer to the reality of privacy and security risks faced by families on a day-to-day basis. Risk from online predators, pedophiles, cyberbullies, cybercriminals, and other online dangers are less likely to occur for younger children due to their small online presence. Parents felt the need to safeguard children by limiting what they could access and who they could talk to online. They exercised a plethora of protection strategies that undermined children's privacy and at times unintentionally jeopardized the children's or their own security. This work highlighted some of the unique challenges faced by parents and children in managing their privacy and security.

Chapter 8

Cyberheroes Interactive Ebook: Design

Cyberheroes[1] is an educational interactive ebook about online privacy that we designed for children under the age of 10. Screenshots and interactive features are documented in Appendix B. The central story is that Cyberheroes (a play on superheroes) with cyberpowers must maintain their secret identities on the Internet. The description of each cyberpower is a privacy-related lesson about personal information, online chatting, location sharing, cyberbullying, and passwords (summarized in Figure 8.4, D).

We used the five-phase ADDIE model introduced in Chapter 5 to develop Cyberheroes. We give a detailed description of our design process using this approach.

8.1 Analysis Phase

The design of our educational interactive ebook Cyberheroes is informed by findings from our Secure Comics study from Chapter 6 and the study on children's privacy models from Chapter 7. Our work on Secure Comics showed that interactive visual narratives increased the persuasive effect of the content and knowledge retention by readers, and has high potential for children's engagement and learning. Our work on children's privacy models showed that children's perception of online privacy is rooted in their understanding of physical privacy, suggesting that risk communication for children should rely on physical analogy and metaphor.

We narrowed our target group to children 7 to 9 years old due to the increasing access to mobile media devices among younger children [143]. Feedback from parents in Chapter 7 also highlighted more concern for the younger children. Furthermore,

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

our literature review in Chapter 4 showed a lack of existing empirically validated resources for children under 10 years old, indicating a need for research in this direction. Children 7 years and older are also appropriate study participants because they are old enough to work more reliably with adults and other children [73].

We selected interactive ebooks as the educational format due to the media's positive learning effects on children, such as improved language and literacy skills [92], increased engagement [88], support for personalized learning [85], and support for reading with adult instruction [153]. We define children's interactive ebooks as digital books with multimodal enhancements such as user-triggered sound, animation, and narration.

8.1.1 Educational Goals

We assumed that our young audience has little to no online experience about privacy. Our aim was to gently introduce the concepts to children without technical and frightening details. Our literature review from Chapter 4 helped to identify privacy and security topics relevant to children. Furthermore, our work on children and parents' perceptions of mobile threats from Chapter 7 suggests that parents are mostly worried about children disclosing personal and location information, talking to strangers, cyberbullying, and poor management of passwords (both by children and other adults). Therefore, the main introductory topics and educational messages included in our interactive ebook are the following:

- Personal information: Children should never provide personal information to anyone on the Internet without asking an adult first. Children were taught to identify seven types of personal information: real name, address, phone number, school, age, birth date, and personal activities (e.g., hobby).
- Online chatting: Children should be careful of whom they trust online because not everyone is who they say they are on the Internet. Children were taught to recognize that people could pretend to be someone else and lie about their true identity.
- Location sharing: Children should never reveal where they are, especially to

strangers. Children were taught that if they share their location on mobile devices, it could reveal to malicious strangers exactly where they are.

- Cyberbullying: Children should be kind and not say mean things on the Internet. Children were taught that if someone says something rude and mean to them, they should not respond, and ask their parents for help.
- Passwords: Children should always keep passwords a secret. Children were taught that the purpose of passwords is to protect secret and precious things.
- Digital trail: Once something is posted on the Internet, it is on the Internet forever. Children were taught that digital information could not be permanently deleted, so they should think carefully about what they post.

These educational messages provided the targets for assessing children's responses to situation-based scenarios in Chapter 9. For example, one of the scenarios for Cyberbullying was "If someone says something rude and mean to you online, what would you do? Why?" The target behaviour was they would not respond, and would talk to their parents.

8.1.2 Entertainment Goals

Since children mainly use mobile devices for entertainment, making the ebook fun and engaging was our second design goal. Slater and Rouner [162] suggest that story appeal, production quality, unobtrusiveness of persuasive subtext, and similarity of characters to self lead to message absorption and engagement in narratives. Privacy and security concepts in our interactive ebook are fully integrated into story to make the educational content seamless from the narrative content. The story was designed to appeal to children with characters that are similar to them. The fantasy storybook illustration style is reminiscent of printed children's picture books.

8.1.3 Conversation-provoking Goals

An early design decision we made was to include parents in children's learning process because our prior work showed that children often relied on parents for advice and guidance in their online interactions, suggesting that children's privacy and security education should involve parents in some way. The ebook functioned as a facilitating tool between the parent and child to promote reflection and discussion around the subject of online privacy. Using the story as a starting point, we wanted the ebook to motivate families to link the subjects presented in the story to their real life experiences and extended the lessons using their own life stories. The intention is to help parents adapt the lessons to their family's needs, concerns, and context.

8.2 Design Phase

8.2.1 Cyberheroes Overview

Narrative: The Cyberheroes interactive ebook was conceptualized based on the idea that Cyberheroes, like superheroes, have secret identities that they must protect. Due to the popularity of the superhero genre through comics and film, we believed the story would resonate with children and make the concept of privacy easy to understand. The story spans across 14 interactive screens and centres around two Cyberheroes, Ally and Bobby, who lost their cyberpowers and must face the consequences. Each cyberpower is privacy lesson identified in the *Analyze Phase* (Section 8.1).

Characters: The ebook was designed to be age, gender, and race inclusive. The main characters 7-year-old Ally and 9-year-old Bobby are the same age as our target audience. Figure 8.1 shows our early character concept sketches. The characters' names were derived from canonical names from security literature, Alice and Bob, used in computer science and engineering scenarios. Ally and Bobby's friends are representative of children from a variety of nationalities (e.g., Figure 8.4, D)

8.2.2 Design Principles

The Cyberheroes interactive ebook applies design principles from persuasive technology (PT) and instructional design (ID) introduced in Chapter 4. Table 8.1 summarizes the implementation of the design principles and indicates which principles were "strongly used" (i.e., full circle), or "weakly used" (i.e., half circle). This distinction indicates that some of the PT principles were strongly used in Cyberheroes while

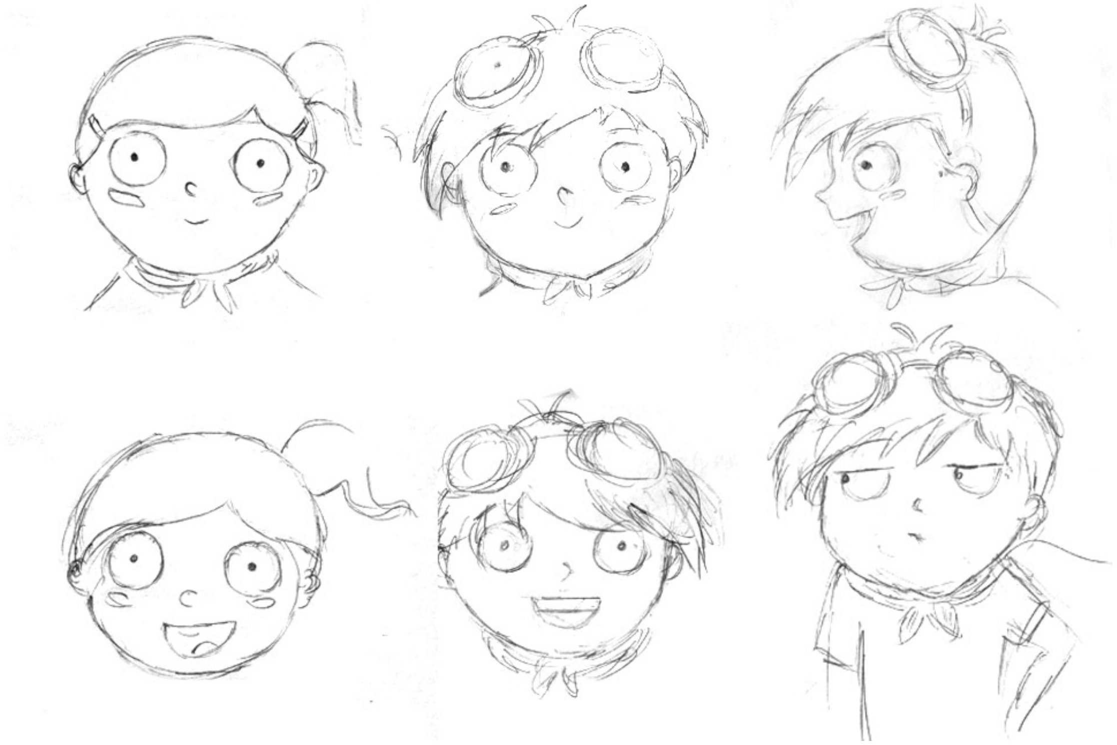


Figure 8.1: Initial character sketches for Ally and Bobby

others were weakly applied. For example, even though the design of Cyberheroes is tailored to children 7 to 9 years old, it does not provide interactive tailoring within the ebook. Therefore, the PT principle of *tailoring* is weakly applied in our work. All ID design principles were strongly used in our design.

Bogost [15] suggests that digital media could rhetorically make arguments through their interactivity. Cyberheroes fuses traditional narrative with interactive aspect to create persuasive experiences, where children interact with the narrative pieces that causes them to think about what is happening to the characters. The application of both PT and ID principles help to achieve our educational, entertainment, and conversation-provoking goals. For example, we used ID principles to break down the lesson content into learner-paced chunks to make it easier to understand. Cyberheroes uses developmentally appropriate means to communicate privacy concepts to children. Children of our target age group tend to focus on only one characteristic at a time [130, 132]. The meet this developmental need, individual screens in the interactive ebook address no more than one point or topic at a time to adhere to the *segmenting* principle. Children press a forward arrow button to advance to the next screen.We used the principle of *reduction* to create short, simple, and actionable educational messages. For example, the interactive ebook provides children with *suggestions* of secure practices by condensing them into five concise Cyberhero rules (Summarized in Figure 8.4, D). Following the *personalization* principle, the interactive ebook is written in child-friendly language. We used simple, direct writing style at a literacy level that is suitable for our target audience, and minimal text. Since children rely on concepts from their physical environment to understand online privacy [191], we used physical security metaphors to communicate abstract online concepts where appropriate. For example, the Internet is a physical place to visit in Cyberheroes, passwords protect a vault that contains Ally and Bobby's favourite toys, and a maze trail allude to digital trails.

To meet our entertainment goals, we used PT principles to *tailor* the content to children. For example, the characters embody *social cues* and physical appearance that are similar to our target age group. The *narrative* is based on the superhero theme that is popular with children. Graphic design is used to establish a visual style that attracts children's attention (see Section 8.3.2). The highly interactive nature of the ebook through *multimedia* helps to create engagement.

Cyberheroes uses PT and ID principles to inspire dialogue between children and parents. Children's interaction with the interface shows *immediate feedback* and cause and effect relationships and consequences of the characters' actions. For example, the "chatting online" screen (Figure 8.4, B) shows that some people online are not who they say they are. When the user taps on the top right character, the image of 9-year-old "Alex" changes to 42-year-old "Mr. R". Ally responds to the change with a surprised expression and a shriek. On the "digital trail" page (Figure 8.4, C), the trail fades away when the user attempts to "erase" it by dragging the pink eraser, but it always reappears, illustrating the difficulty of removing online content once posted. These feedback loops prompt children to ask questions and discuss with parents about what is happening in the story. The interaction also helps to achieve *procedural rhetoric*. In the first example, the rhetorical argument made through interactivity is that people could lie about their real identities on the Internet so children should be careful of whom to trust. In the second example, rhetorical argument is that online content cannot be permanently removed, so children should think about the potential consequences before they post.

For usability, the interactive ebook is optimized for high-resolution retina iPad screens to ensure a large reading surface. All visual interactive objects have a sizeable hotspot to facilitate selection. Large fonts are used for readability. Interactive elements have clear affordances and are visually marked to be easily distinguishable from the non-interactive elements. For example, interactive objects that enable tapping are visually mapped with a rotating star and draggable objects are visually mapped with a directional pulsing hand symbol (Figure 8.4, C). These translucent "help" markers do not obstruct the images below, and fade away after activation. To reactivate the markers, users could select the "star" icon from the menu, or return to the screen.

8.3 Development Phase

8.3.1 Content Development

We first wrote the Cyberheroes story and determined that each screen should contain no more than 2 to 3 sentences to keep the textual information brief. The script was iterated several times to ensure the narrative flow while keeping important educational content intact. Once we determined the narrative structure, we created storyboards and planned the user interaction. The character design and storyboards were iterated after receiving feedback from members of our lab, other graphic designers, and elementary school teachers. For example, Figure 8.2 shows one of the storyboards where Ally and Bobby transform into cyberheroes. Feedback from others suggested that both characters should wear masks to clearly communicate the protection of their identity. Furthermore, characters' monograms on their costumes should avoid stereotypes (e.g., heart symbol for girls). These changes were made in the final design.

The storyboards functioned as a guide for the final visual design. We played with the composition and added more details from the original concept to the final design.

PT & ID Principles	Used	Implementation
Reduction	◐	Colourful illustrations and minimal text account for children's limited attention and vocabulary.
Tunneling		
Personalization		
Conditioning	◐	Children receive motivating superhero-themed voiceovers such as "Fantasrific!", "Ok! Here we go!", or "Super!"
Suggestion	●	A list of five Cyberhero rules suggest good online practices. For example, "the third Cyberhero rule is to never reveal where you are, especially to strangers."
Tailoring	◐	Cyberheroes is tailored to children 7 to 9 years old.
Social Cues	●	The characters are the same age as the target audience. They persuade children to follow their example.
Simulation		
Monitoring		
Rehearsal		
Procedural Rhetoric	◐	Rhetoric is achieved through interaction with the story content. For example, when children tap on the top-right character on the 'online trust' page (Figure 8.4, B), the image of 9-year-old 'Alex' changes to 42-year-old 'Mr. R'. Ally responds to the change with a surprised expression and a shriek.
Segmenting	●	Individual screens address no more than one point or topic.
Contiguity	●	All text in the interactive ebook is given careful typographic consideration to ensure that they work with the illustrations.
Reflection	●	Interactive elements cause reflection through interaction. For example, on the 'digital trail' page (Figure 8.4, C), the trail fades away when the user attempts to "erase" it by dragging the pink eraser, but it always reappears, illustrating the difficulty with removing online content once posted.
Immediate Feedback	●	The interface respond to children's input with sounds, animation, and image alterations.
Narrative	●	The story revolves around Cyberheroes Ally and Bobby who lost and regain their Cyberpowers.
Signalling	●	The interface is simple with visual cues to highlight the interactive areas on screen (marked with a rotating star or a pulsing hand symbol for movable objects). Important words in the narrative are enlarged to emphasize their importance.
Socialization	●	The interactive ebook gives advice in child-friendly language speaking directly to the reader (e.g., "be careful who *you* trust online").
Multimedia	●	The interactive features, animations, and sound show cause and effect relationships, advance the story, or infer moods and feelings of the characters or the situation.
Conceptual-Procedural	●	The interactive ebook aims to provide children with conceptual knowledge. Procedural knowledge is supplemented by parents through co-reading.

Table 8.1: Design principles implemented in Cyberheroes. ● = strongly uses the principle; ◐ = weakly uses the principle; *no circle* = does not use the principle.

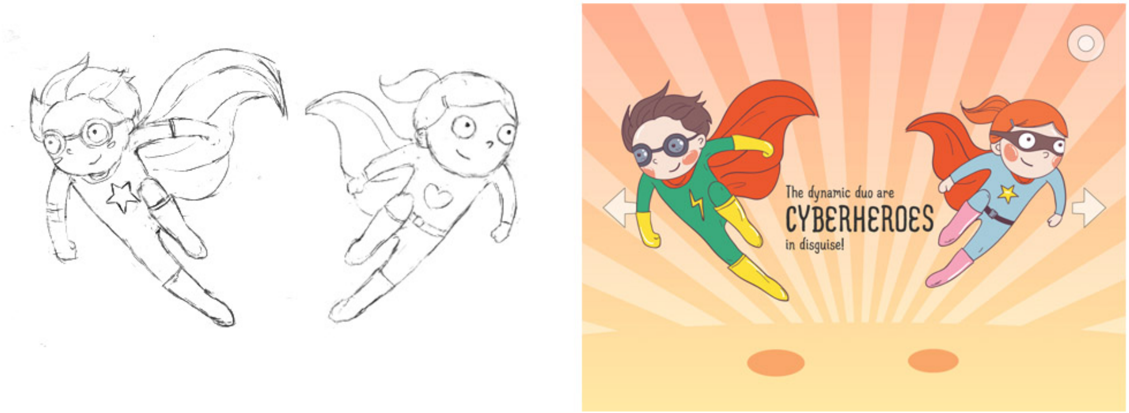


Figure 8.2: Ally and Bobby's costumes were refined from the storyboard concept (left) to the final design (right)

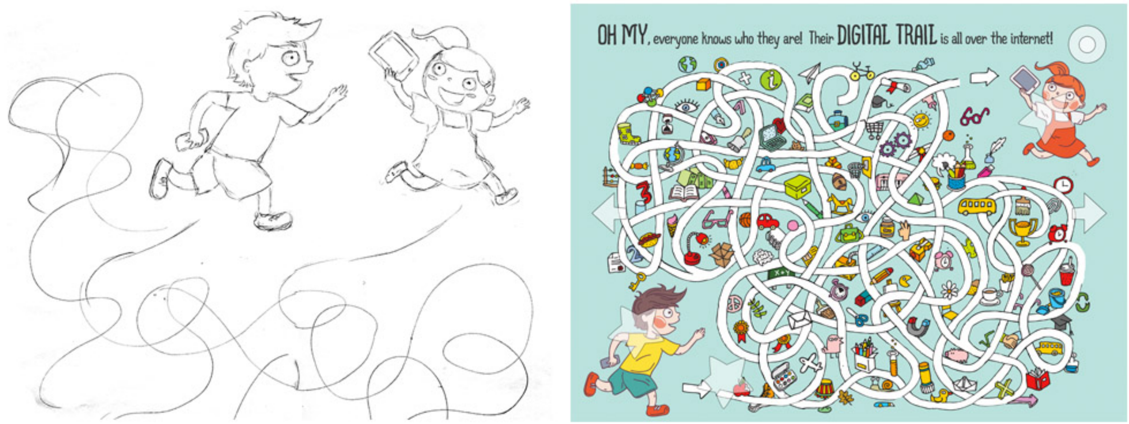

OH MY, everyone knows who they are! Their DIGITAL TRAIL is all over the internet!

Figure 8.3: One of the early storyboards (left) and the final screen (right).

Figure 8.3 shows how we transformed a simple line drawing to the detailed final screen to portray the digital trail left by Ally and Bobby. To increase readability, we used large fonts and emphasized certain words to highlight their importance.

Interactive Features: The story spans across 14 screens with interactive features, animation, and sounds. The interactive features are large enough to facilitate easy selection, and require only simple interactions suitable for children such as tapping and drag-and-drop. A detailed mapping of the start state and the active state of each screen is included in Appendix B.

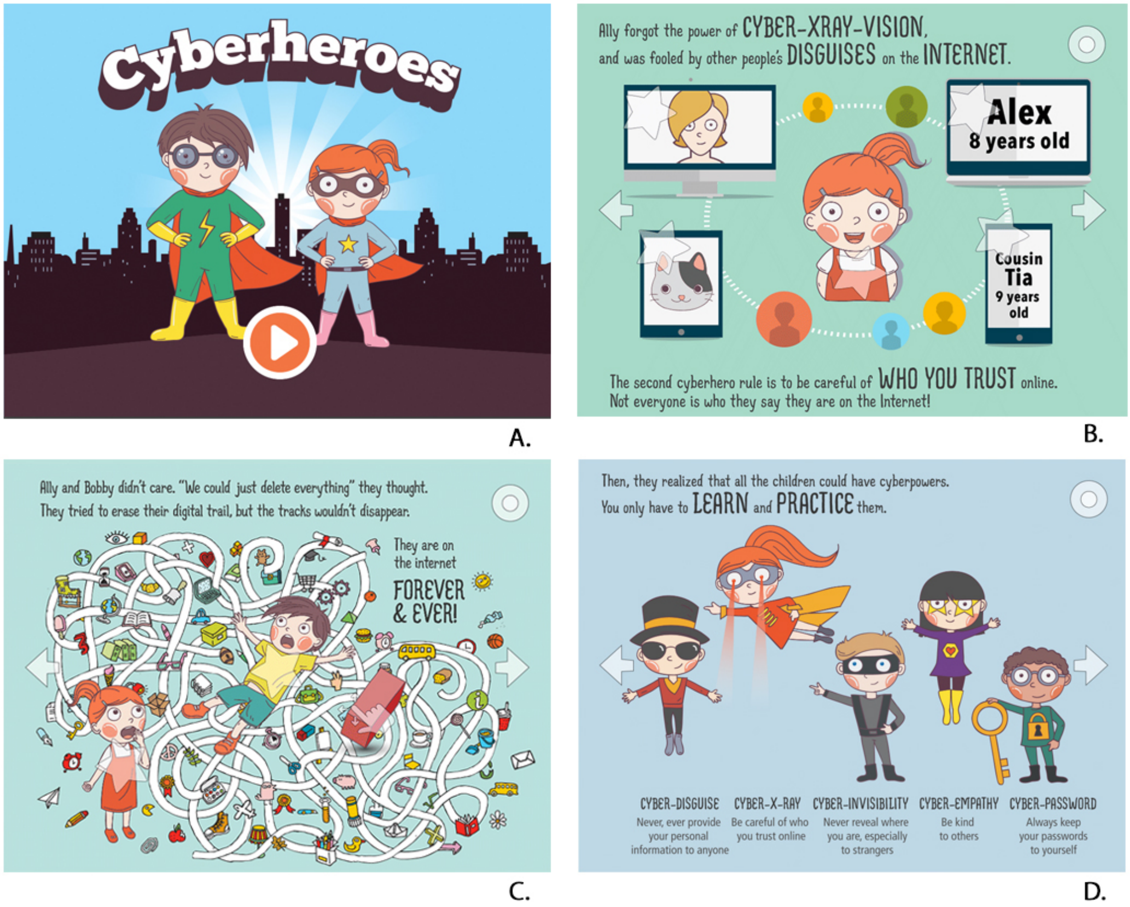

Cyberheroes
A.
Ally forgot the power of CYBER-XRAY-VISION,
and was fooled by other people's DISGUISES on the INTERNET.
Alex
8 years old
Cousin
Tia
9 years
old
The second cyberhero rule is to be careful of WHO YOU TRUST online.
Not everyone is who they say they are on the Internet!
B.
Ally and Bobby didn't care. "We could just delete everything" they thought.
They tried to erase their digital trail, but the tracks wouldn't disappear.
They are on
the internet
FOREVER
& EVER!
C.
Then, they realized that all the children could have cyberpowers.
You only have to LEARN and PRACTICE them.
CYBER-DISGUISE
Never, ever provide
your personal
information to anyone
CYBER-X-RAY
Be careful of who
you trust online
CYBER-INVISIBILITY
Never reveal where
you are, especially
to strangers
CYBER-EMPATHY
Be kind
to others
CYBER-PASSWORD
Always keep
your passwords
to yourself
D.

Figure 8.4: Sample screens and interactions from Cyberheroes. A) Home Screen: the user presses the "play" button to start playing; B) Talking Online: the user taps on the screen characters to reveal their real identity, and Ally reacts; C) Digital Trail: the user drags the pink eraser over the digital trail to "erase" it, then the trail reappears; D) Cyberpowers: the user taps on each character to transform them into Cyberheroes. Each characters has an associated animation and audio clip as they transform.

8.3.2 Graphic Design

To determine an appropriate visual style for our target audience, we explored local libraries and bookstores. Children's books are typically sorted by age. This enabled us to easily identify the style of popular short story picture books available to children aged 7 to 9. From this exercise, we determined the main visual design elements for our interactive ebook.

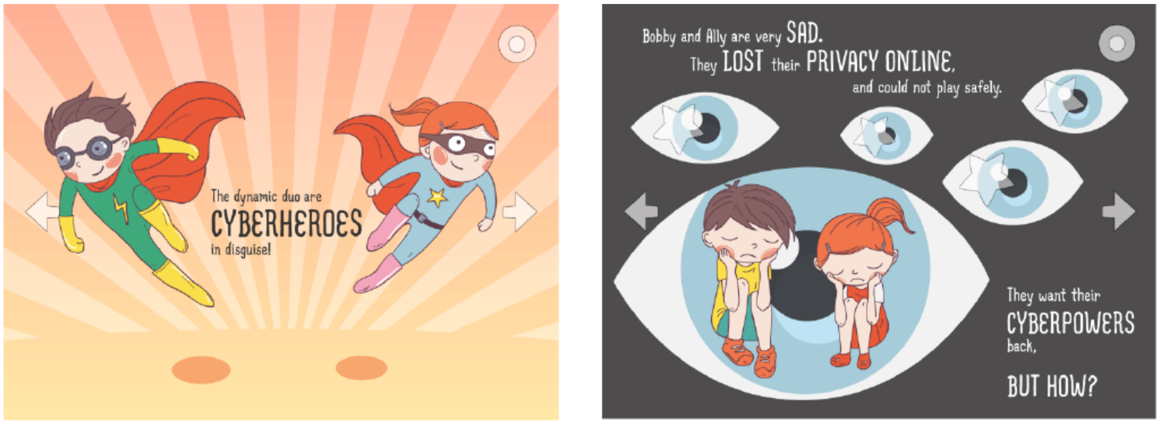

The dynamic duo are
CYBERHEROES
in disguise!
Bobby and Ally are very SAD.
They LOST their PRIVACY ONLINE,
and could not play safely.
They want their
CYBERPOWERS
back,
BUT HOW?

Figure 8.5: Warm bright colours are used to portray happiness (left), and cool dark colours are used to portray sadness (right).

Bright, Vivid Colours, and a Happy Mood: Like traditional printed children's picture books, our interactive ebook uses bright, vivid colours that stimulate the senses and capture children's attention. Research show that children tend to be attracted to bright blocks of colour rather than pastels and neutrals [33]. Furthermore, primary colours (red, yellow, blue), and secondary colours (green, orange, purple) are the most appealing to children. These colours tend to stand out more in children's field of vision, and appears to be more stimulating and interesting than muted colours [17].

Colour has been found to affect children's moods and emotions [17]. They associate warm bright colours like red, and orange and yellow to happiness and comfort and dark cool colours like black and grey to more negative emotions. To make a big impression on children, Cyberheroes used a bright and vivid colour palette. Furthermore, colour is carefully selected to infer moods and emotions of the story. For example, when the characters transform into Cyberheroes, we applied a happy, energetic colour palette of orange, yellow, and pink (see Figure 8.5, left). When the characters are sad, we applied a cool and muted colour palette of blue and grey (see Figure 8.5, right).

Large Design Elements: Large interface design elements have proven to be effective for children [68]. They draw children's attention to recognizable objects, increase selection accuracy, and improves the simplicity and usability of the interface [68]. Our aim for Cyberheroes is to create design elements that are large and visually memorable. These include oversized typography, large buttons, sizeable call-to-action areas, and big graphics. We chose a friendly-looking, condensed hand-drawn typeface with a playful vibe called *Prova* to compliment the illustration work. The buttons are designed to be big and simple. Interactive objects have much larger active hotspots that are invisible underneath the "star" markers to ensure easy selection. For example, on the right screen in Figure 8.5, tapping anywhere on the eye graphics cause them to blink. Lastly, we used big graphics with splashes of bold colours for visual impact.

Children prefer character designs with round faces, large heads, and big eyes, a phenomenon ethologists called the "baby schema", which states that high infantile traits (i.e., baby-like traits that induce cuteness) in people and animals are highly appealing for humans [16]. Characters in Cyberheroes are designed to embody these traits to appear friendly and cute.

8.3.3 Navigation

Cyberheroes enables children to start reading by pressing a large animated play button on the landing screen. Children navigate the screens sequentially by tapping on a forward or backward arrow button. We avoided swiping gestures for page-turning because the motion requires some precision that could be tricky for small fingers. Interactive objects that enable tapping are visually mapped with a rotating star and draggable objects are visually mapped with a directional pulsing hand symbol (Figure 8.4, C) to make them easily distinguishable from the non-interactive elements. The circular icon at the top corner of the screen expands/collapses a three-item menu to enable users to go the home screen, hide/show the interactive markers, or disable/enable all sounds. We avoided the use of the bottom area of the screen entirely for navigation purposes because children could easily touch the bottom of the tablet by accident.

8.4 Implementation Phase

We drew the illustrations for Cyberheroes in Adobe Illustrator CS6 using a Wacom Intuos Graphics Pen and Touch tablet. Pencil sketches were first created on paper, then scanned and imported to Illustrator to produce the vector-based drawings, and

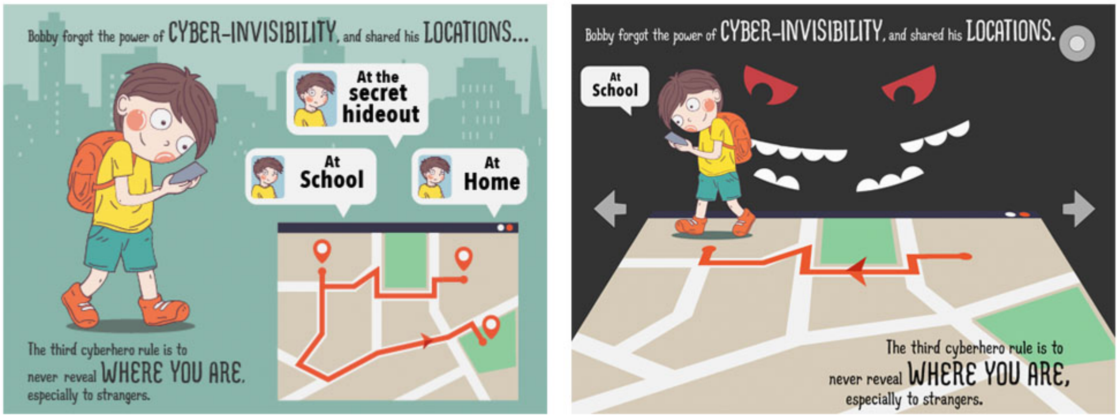

Bobby forgot the power of CYBER-INVISIBILITY, and shared his LOCATIONS...
At the secret hideout
At School
At Home
The third cyberhero rule is to never reveal WHERE YOU ARE, especially to strangers.
Bobby forgot the power of CYBER-INVISIBILITY, and shared his LOCATIONS.
At School
The third cyberhero rule is to never reveal WHERE YOU ARE, especially to strangers.

Figure 8.6: Location sharing screen was further iterated during implementation from the original concept (left) to the final screen (right)

to colour the artwork. Some backgrounds were adapted and recoloured from stock images downloaded from Shutterstock. In some cases, we further iterated the concept. For example, we initially designed the location sharing screen with an image of Bobby walking in the background while showing an interactive map image to display Bobby's location each time the user taps on the map (see Figure 8.6, left). However, after further assessment, we decided that the map concept might be too abstract for children to perceive the consequences. We improved the design by overlaying the movement of Bobby on top of the map to show a direct connection between the two (see Figure 8.6, right). A menacing gaze follows Bobby's every movement as he goes from home, to school, and finally, to his secret hideout.

Graphics were imported into GameSalad Creator (the same developer tool we used for Secure Comics) to create the interactive features. The application enabled us to apply a wide range of interaction behaviours such as movements, collisions, animation, and sounds. We used over 30 sound effects and 13 pre-recorded voice effects from `freesound.org`, and 10 theatrical music scores from `audioblocks.com` for the background music. Cyberheroes was optimized for high-resolution retina displays and released to the public as an app in the Apple Store[2], and as a HTML5 web comic[3].

[2] https://itunes.apple.com/ca/app/cyberheroes/id1095724919

[3] http://www.versipass.com/edusec/cyberheroes/app/app.html

8.5 Evaluation Phase

We evaluated Cyberheroes with children 7 to 9 years old, and their parents. We describe our methodology and research findings in the next chapter.

Chapter 9

Cyberheroes Interactive Ebook: Evaluation

In this chapter, we show that Cyberheroes makes learning engaging, comprehensible, and memorable for children, and creates discussion opportunities with parents. To the best of our knowledge, this work is the first research-driven study on designing and evaluating a privacy educational tool and showing empirical evidence of significant learning effects on children's privacy knowledge and behaviour. The work presented in this chapter has been submitted to the International Journal of Child-Computer Interaction (IJCCI) in 2016 and is currently in revision.

9.1 Methodology

In our between-subject study, the dependent variables are *privacy knowledge* and *privacy behaviour*, and the independent variable is the type of media (i.e., the Cyberheroes interactive ebook and a text-only version of the same narrative as the control). Similar to the methodology used for Secure Comics in Chapter 6, children's responses to situation-based scenarios were used to measure behaviour because it would be unreasonable and unethical to place children in real compromising online situations. The scenarios were not based the educational content, but describe independent situations designed to test children's ability to apply the learned information to different contexts.

The study design is based on the between-subject pre-test, post-test, followup (PPF) design used in the Secure Comics study from Chapter 6 (Section 6.1). Child-parent pairs were pseudo-randomly assigned to follow either the *ebook* or the *text* group procedure outlined in Table 9.1. The experiment took two sessions conducted a week apart and lasting approximately 40 minutes for session 1 and 15 minutes for session 2. The dependent variables were measured pre-reading (Pre-Test), post-reading (Post-Test), and a third time 1-week post-reading (1-week-Test). The *ebook* group was provided with 2 iPads and the *text* group was provided with 2 letter-sized printouts. Both groups were given full control of the co-reading sessions.

Our researcher questions were: 1) Do the groups differ in privacy knowledge and behaviour from the pre-test to the post-test? 2) Do the groups differ in privacy knowledge and behaviour from the pre-test to the one-week-test? 2) Do the groups differ in privacy knowledge and behaviour from the post-test to the one-week-test?

9.1.1 Text Control

We repeated our methodology from Chapter 6 and used text as the control condition. Text provided the most basic form of the educational content included in Cyberheroes and enabled us to convey the same narrative without the visuals, interaction, animation, and sound. Cyberheroes was designed to be read together with an adult, and text enabled a more similar reading format to interactive ebooks compared to other media like film and animation. Additionally, adults could provide assistance to children if they have any difficulties reading.

We took care to ensure that the text-only version read like a children's storybook and retained the same imaginative narrative flow as Cyberheroes. Both versions also contained identical educational information. To increase the narrative quality, we added descriptive information in the text-only version to describe the scene and connect the narrative pieces. For example, on the online chatting screen, children who participated in the *ebook* procedure interacted with the screen shown in Figure 8.4, B, while children who participated in the *text* procedure read the following text segment:

> Ally forgot the power of Cyber-Xray-Vision, and was fooled by other people's disguises on the internet. Ally talked to:
>
> - Aunt Peggy (42 years old)
> - Alex (8 years old). He is actually Mr. R (47 years old).
> - Kitty (age unknown). She is actually Erin (36 years old).
> - Cousin Tia (9 years old).
>
> The second cyberhero rule is to be careful of who you trust online. Not everyone is who they say they are on the Internet!

Procedure & Materials			
Ses.	**Participants**	**Ebook Procedure**	**Text Procedure**
I	Parent	A) Demographic Questionnaires	A) Demographic Questionnaires
	Child	B) Pre-Test Interviews	B) Pre-Test Interviews
	Parent&Child	Co-read interactive *ebook*	Co-read narrative *text*
	Parent	C) Adult Usability Questionnaire	N/A
	Child	C) Child Usability Questionnaire	
		B) Post-Test Interviews	B) Post-Test Interviews
1-week Interval			
II	Child	B) 1-Week-Test Interviews	B) 1-Week-Test Interviews
	Parent&Child	N/A	Co-read interactive *ebook*
	Parent		C) Adult Usability Questionnaire
	Child		C) Child Usability Questionnaire

Table 9.1: Summary of the study procedure. The colours group similar activities together. Materials are described in Section 9.1.3

The full text for the control condition is included in Appendix E.8. Screenshots of Cyberheroes and its interactive features are documented in Appendix B.

9.1.2 Participants and Recruitment

The sample included 22 child-parent dyads with 14 girls and 8 boys between the ages of 7 to 9 (Mean = 8). To minimize the effects of gender differences, the sample is balanced with seven girls and four boys per group. Children's mean age is 8.1 years in the *ebook* group and 7.9 years in the *text* group. Participation was restricted to one child per family who used a mobile device regularly. None of the children had prior formal privacy education. Nineteen mothers and three fathers accompanied the children. The parents were between the ages of 30 to 44 and from a wide range of socio-economic backgrounds and education levels, including bachelor's degree (n = 10), college diploma (n = 6), high school diploma (n = 3), and Masters degree (n = 3). Six mothers were stay-at-home moms; others worked in education (n = 5), social services (n = 4), business (n = 2), healthcare (n = 1), and food services (n = 1). The three fathers worked in healthcare, business, and education.

After receiving clearance from our Research Ethics Board, invitations were shared with parents in the cities of Kitchener-Waterloo and Cambridge, ON., Canada through public parenting groups on social media. Emails of our recruitment notice were also forwarded to parents by local education resource centres.

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

9.1.3 Evaluation Measures

The evaluation measures were administered according to the study procedure outlined in Table 9.1 and correspond to the letter codes listed. All study material is included in Appendix E.

A) Demographic/Activities, Pre-Evaluation Questionnaires: All 22 parents completed an Adult Demographic Questionnaire (age, gender, education, occupation). They completed a Child Demographic & Activities Questionnaire for their children. The demographic portion contained children's age, gender, and grade. The activities portion asked about children's daily device use, the types of devices used, and online activities. Lastly, we inquired whether children had prior experience reading interactive e-books and privacy education.

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

B) Children's Privacy Proficiency Tests: We designed each privacy proficiency test to contain four knowledge-based questions and six behaviour-based questions assessing children's overall proficiency to practice privacy-conscious behaviour. Our knowledge-based questions inquired about children's understanding of privacy and personal information (e.g., what it is, how to protect it, what could happen if people had no privacy). To test children's behaviour, they responded to situation-based scenarios on the topics of personal information, online chatting, location sharing, cyber-bullying, passwords, and digital trail. Children responded to each scenario by explaining what they would do and why. For example, the pre-test scenario for passwords is: *Your best friend wants to borrow your password to email a funny picture to a friend that you both know. What would you do? Why?* The pre-tests established a baseline for each child, and the questions were repeated verbatim in the post-tests. The 1-week-tests evaluated the same concepts but contained alternate scenarios. The tests were administered as interviews, which is an appropriate data collection method for children 7 years and older that has several benefits over surveys, including reducing fatigue, increasing attention, and enabling the researcher to prompt children for further information if the answers are unclear or vague [152]. Our interviews with children were audio recorded and transcribed.

C) Child & Parent Usability Questionnaires: The child questionnaire contained eight questions. We first measured engagement using an Again-Again Table [139] asking: *1) Would you read Cyberheroes again?*. Next, children answered five questions using the 5-point Smileyometer [139] (i.e., visual Likert-scales): *2) How fun was the Cyberheroes ebook? 3) How easy was it to use the Cyberheroes ebook? 4) How well did you learn from the Cyberheroes ebook? 5) How likeable were Ally and Bobby? 6) How willing would you be to show the Cyberheroes ebook to other kids?* In the analysis, the Again-Again Table evaluations were coded as 3 for "yes", 2 for "maybe" and 1 for "no". The Likert-scale questions were coded from 1 for least positive, to 5 for most positive. Lastly, children answered open-end questions: *7) What did you like about the Cyberheroes ebook? 8) What did you dislike about the Cyberheroes ebook?*

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

We wanted make the study experience fun for families and give both the *text* and *ebook* groups the opportunity to view and evaluate Cyberheroes. The usability evaluation procedure is designed to not confound the results of children's privacy proficiency tests. Both the *text* and *ebook* conditions completed the privacy proficiency tests first, then the *text* group was allowed to also experience the Cyberheroes interactive ebook and complete the usability evaluation at the end of the study (see Table 6.1). Results in Section 9.2.3 suggest no statistically significant differences in children's opinions of Cyberheroes between groups.

9.1.4 Data Analysis

Interviews: The transcriptions of the audio-recorded responses were organized in Excel according to the interview questions. The primary researcher and a graduate research assistant who helped to conduct the user study and transcription coded all responses independently based on a pre-agreed answer key. A score of 3 is allocated for an "excellent response", 2 for a "marginal response", and 1 for a "poor response". The researchers worked together to establish the answer key based on the target behaviours that were taught to children in the interactive ebook. For example, in the event of cyberbullying, Cyberheroes taught children to not respond, walk away, and talk to their parents. During their privacy tests, we asked children what they would do if a friend said something rude and mean to them (the alternate scenario in the 1-week-test is someone said something mean to a friend). Children's responses that met the target behaviours from ebook received a score of 3. Children who responded to the mean message and chose not to talk to their parents received a score of 1. Partially correct behaviours, such as when children decided to walk away after responding back to the mean message received a score of 2. The interviews were scored out of 12 points for *privacy knowledge*, and 18 points for *privacy behaviour* on each test. The two scores were then added to obtain children's total privacy proficiency score for a maximum of 30 points. A Cohen's Kappa (k) test showed very strong agreement between the two researchers' analysis of the Pre-Test (k = 0.972, 95% CI: 0.945 to

0.999, $p < 0.001$), Post-Test ($k = 0.977$, 95% CI: 0.952 to 1.000, $p < 0.001$), and 1-Week-Test ($k = 0.947$, 95% CI: 0.908 to 0.986, $p < 0.001$). In cases of disagreement, mean scores between the two researchers were used in the analysis.

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

9.2 Children's Privacy Tests Results

As recommended by Rausch et al. [136], we used with one-way Analysis of Covariance (ANCOVA) tests to interpret whether there are differences in children's post and 1-week privacy scores between the two conditions after controlling for pre-existing knowledge and behaviour using children's pre-test scores as a covariate. Additionally, we tested children's 1-week privacy scores between the two conditions after controlling for their learned knowledge and behaviour using children's post-test scores as a covariate. The results are summarized in Table 9.2 and visualized in Figure 9.1. The unadjusted and adjusted means used in the analysis are summarized in Table 9.3.

The assumptions for the ANCOVA were met: Visual inspection of two scatterplots shows a linear relationship between the Pre-/Post-Tests scores, and between the Pre-/1-Week-Tests scores for each condition. There was homogeneity of regression slopes as the interaction term between the Pre-/Post-Test and Pre-/1-week-Test were not statistically significant. Standardized residuals for the readings and for the overall model were normally distributed, as assessed by Shapiro-Wilk's test. There was homoscedasticity as visually assessed by a scatterplot of the standardized residuals plotted against the predicted values, and homogeneity of variances by running a Levene's test. No outliners exist in the data, as standardized residuals did not exceed ±3 standard deviations.

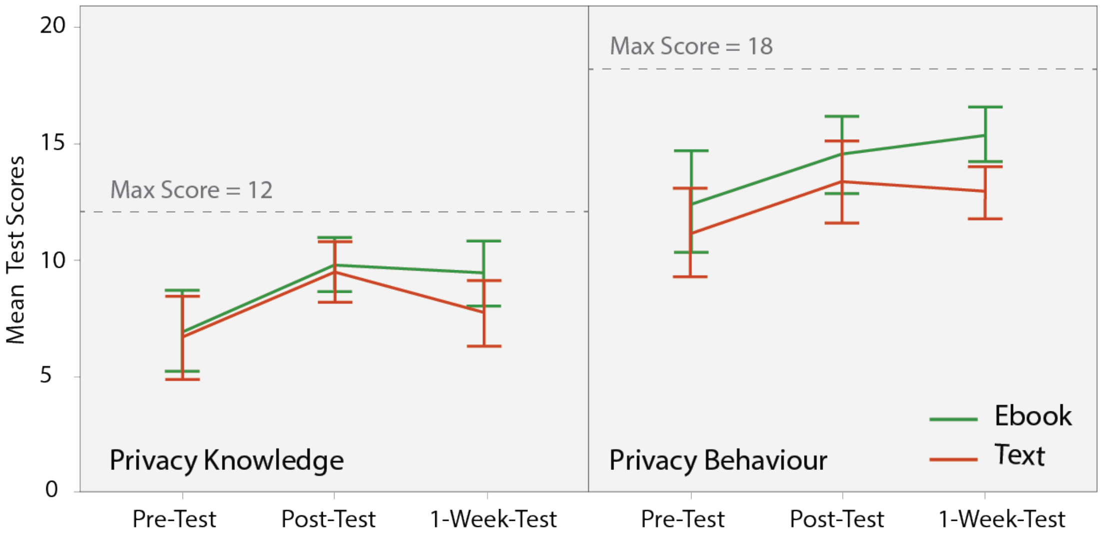


Figure 9.1: Summary of children's pre-, post-, and one-week-test scores between groups. Error Bars: 95% Confidence Interval (CI)

Privacy Knowledge			
Tests	MD	95% CI	p
Pre/Post	.2	[-1.3, 1.5]	.826
Pre/1-week	1.5	[.01, 3.0]	**.044**
Post/1-week	1.5	[-.04, 3.0]	**.054**
Privacy Behaviour			
Pre/Post	.3	[-1.3, 1.8]	.735
Pre/1-week	2.0	[.7, 3.1]	**.003**
Post/1-week	2.0	[.7, 3.1]	**.003**

Table 9.2: ANCOVA tests showing statistically significant difference between groups for *privacy knowledge* in the Pre/1-Week-Test and the Post/1-Week-Test. A statistically significant difference between groups for *privacy behaviour* was found in the Pre/1-Week-Test and the Post/1-Week-Test. MD = Mean Difference, CI = Confidence Interval, p = Significance Level.

Between-Subject Effects on Privacy Knowledge: Using the adjusted means of children's knowledge scores in Table 9.3, the results revealed no statistically significant difference in the Post-Test scores between the conditions. In other words, children in both conditions increased their *privacy knowledge* after reading. One week later however, there was a statistically significant difference in the 1-Week-Test *privacy knowledge* scores between the conditions, $F(1, 19) = 4.7$, $p < .05$, partial $\eta^2 = .197$. 1-week *privacy knowledge* was greater in the *ebook* group than in the *text* group.

Privacy Knowledge						*Privacy Behaviour*			
		Unadjusted		Adjusted		Unadjusted		Adjusted	
Tests	Condition	M	SD	M	SE	M	SD	M	SE
Pre/Post	Ebook	9.7	1.8	9.7	.5	14.5	2.6	14.1	.5
	Text	9.5	2.0	9.5	.5	13.5	2.7	13.9	.5
Pre/1-Week	Ebook	9.4	2.1	9.3	.5	15.4	1.8	15.2	.4
	Text	7.7	2.1	7.8	.5	13.0	1.7	13.3	.4
Post/1-Week	Ebook	9.4	2.1	9.3	.5	15.4	1.8	15.2	.4
	Text	7.7	2.1	7.8	.5	13.0	1.7	13.3	.4

Table 9.3: Adjusted and unadjusted means and variability for the Post-Test and 1-Week-Test privacy proficiency scores with Pre-Test privacy proficiency scores as a covariate, and 1-Week-Test privacy proficiency scores with Post-Test privacy proficiency scores as a covariate. Adjusted means are used in the analysis. M = Mean, SD = Standard Deviation, SE = Standard Error.

There was also a significant difference between groups in the post- vs. 1-week tests, $F(1, 19) = 4.2$, $p = .05$, partial $\eta^2 = .179$, showing that the *ebook* was significantly more successful than *text* at sustaining *privacy knowledge* after one week.

Between-Subject Effects on Privacy Behaviour: Using the adjusted means of children's behaviour scores in Table 9.3, we found a statistically significant difference between groups one week later, $F(1, 19) = 11.7$, $p = .003$, partial $\eta^2 = .380$, but no statistically significant difference immediately after reading. The *ebook* was more successful than *text* at sustaining children's *privacy behaviour* from the post-test to the one-week-test.

9.2.1 Children's Privacy Tests Results Summary

Both the interactive ebook and the text-only narrative format improved children's privacy knowledge and behaviour immediately after reading. However, a comparison of the two conditions showed that the *ebook* group maintained higher scores for *privacy knowledge* and *privacy behaviour* after one week, even when adjusted for variance in baseline knowledge and behaviour. The Cyberheroes interactive ebook therefore appears more effective than the text-only format at maintaining 1-week learning effects on children's privacy knowledge and behaviour.

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

Table 9.4: Parent-child total co-reading time, time spent on privacy discussions, and co-reading formats. 'P' = Parent, 'C' = Child. Time is shown in minutes.

9.2.2 Co-reading Interactions

Parent-child co-reading time, duration of privacy discussions, and reading format are summarized in Table 9.4. Both groups showed various co-reading preferences. The narrative stimulated parents in both groups to ask children questions such as, "what do you think is the difference between a cyberhero and a cybervillain?" (P3-ebook), or "if cyberheroes are the good people who are the cybervillains?" (P6-text). The children would give responses such as "the heroes try to save all the privacy" (C3-ebook), and the cybervillains are "the bad people" (C6-text). However, the interactive ebook motivated more meaningful discussions through interactions with the interface. The interactive ebook prompted 2:02 minutes of child-parent discussions compared to 59 seconds for the control. Children asked parents questions while referring to onscreen text, images, and interactions, while the *text* group solely relied on the story. Children used all interactive features, and two children read parts of Cyberheroes more than once. Children spent the longest time on online chatting (Figure 8.4, B), personal information, and cyberpowers (Figure 8.4, D), and interacted with the content multiple times to activate sound effects and animations, suggesting these screens were the most engaging for children. To demonstrate the types of child-parent interactions that took place, we give P8-ebook and C8-ebook's conversation while using the online chatting screen as an example:

- The child taps on a character on screen who appeared to be 8-year-old Alex, but the image changed to 42-year-old Mr. R.
  - Parent: *"So he's not Alex, he's Mr. R, so he is lying; he is using a disguise."* [The parent points to another character.] *"So is that aunt Peggy?"*
  - Child: [Taps the character and the image changed to aunt Peggy] *"Yup!"*

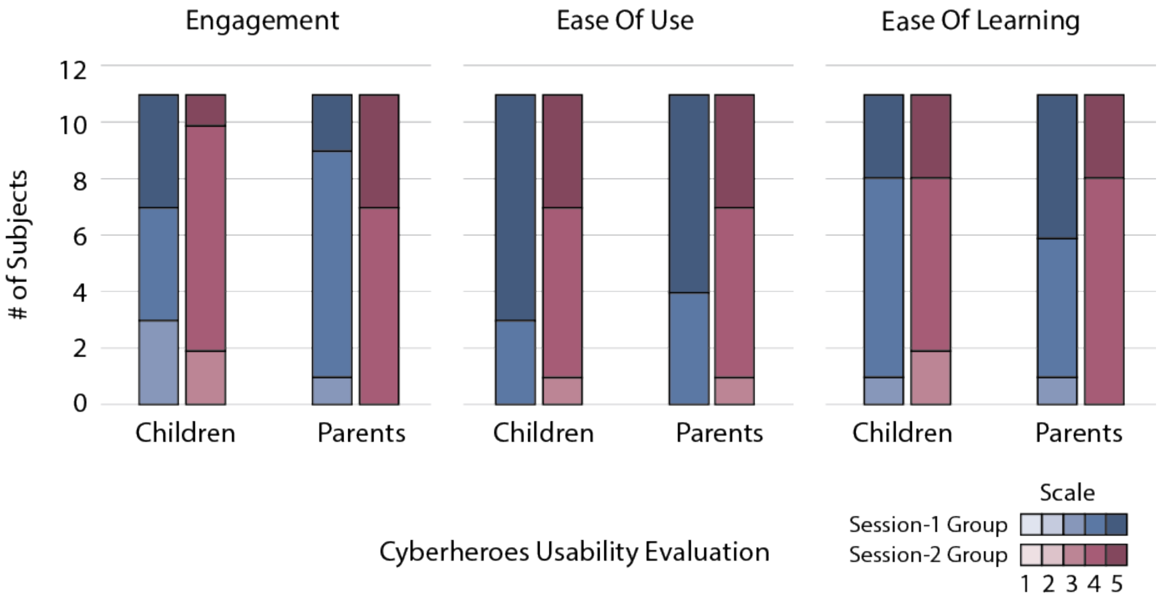


Figure 9.2: Summary of children and parents' usability evaluations of the Cyberheroes interactive ebook on engagement, ease of use, and ease of learning on a 5-point Likert-scale, where 5 is most positive.

- Parent: [The parent points to another character] *"Is that kitty?"*
- Child: [Taps the character and the image changed to 36-year-old Erin] *"Uh, it's not."*
- Parent: *"That's Erin, she's 36 years old and she's pretending to be a cat."*
- Child: *"So those two are liars and those two are true friends."*

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

9.2.3 Usability of Cyberheroes

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

We did not find gender effects or between-group effects in the usability evaluations of Cyberheroes. Mann-Whitney U tests showed no statistically significant differences between gender (Engagement: $U = 39, Z = -1.285, p = .199$; Ease of Use: $U = 54, Z = -.155, p = .876$; Ease of Learning: $U = 29.5, Z = -2.058, p = .070$), or between conditions (Engagement: $U = 52, Z = -.618, p = .537$; Ease of Use: $U = 37, Z = -1.758, p = .079$; Ease of Learning: $U = 56.5, Z = -.299, p = .765$). However, to avoid possible bias caused by the *text* group's reading of the text-only format prior to reading the interactive ebook, we present the usability results between the two groups independently. In the following section, we refer to children and parents who read the ebook in the first session as the "session-1 group", and those who read the ebook in the second session as the "session-2 group". Usability evaluations of Cyberheroes from all 22 children and 22 parents were consistently positive. Figure 9.2 shows a comparison of their evaluations on "engagement", "ease of use", and "ease of learning".

Cyberheroes is engaging for children. The Smileyometer and the Again-Again Table from the Fun Toolkit [139] were used to measure engagement. Reed and MacFarlane [139] found high correlations between them for measurements of engagement (i.e., fun), suggesting that they are assessing the same construct.

Results from the two instruments showed that children found Cyberheroes fairly engaging. Figure 9.2 shows their Smileyometer evaluations for engagement. Furthermore, the Again-Again Table evaluations showed a mean score of 2.27/3 for the session-1 group ($n = 3$ for "yes", $n = 8$ for "maybe", $n = 0$ for "no") and 2.45 for the session-2 group ($n = 6$ for "yes", $n = 4$ for "maybe", $n = 1$ for "no"). Other aspects of the evaluation showed that children found the characters likeable (session-1 and session-2 groups: $M = 3.82$), and were willing to recommended Cyberheroes to others (session-1 and session-2 groups: $M = 3.82$). Open-ended feedback suggested that children highly enjoyed the interactive features and the superhero theme. They particularly liked "pressing the stars"[1] to show cause and effect relationships. For example, C6-ebook said, I liked "pressing the stars because we could figure out if they are good guys or bad guys." Children liked that at the end of the story "everyone became cyberheroes" (C7-text).

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

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

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

Parents also thought Cyberheroes was an effective learning tool for children. The ebook was a "good introduction to the concepts, basic enough to prompt the child to

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

ask for more information and details about what's going on" (P6-ebook). It "introduced danger without scaring them" (P10-ebook), and achieved explaining privacy at an elementary level that is very attractive to children, which "increased their interest to read to the end of the story" (P8-text).

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

9.3 Discussion

The results of this study with 7 to 9-year-old children are fairly consistent with our study of Secure Comics with 11 to 13-year-old children in Chapter 6. Both Cyberheroes and Secure Comics improved children's motivation to practice secure actions post and one week after reading, and both studies showed an improvement in children's privacy knowledge; their ability to explain why practicing certain behaviours are necessary to protect their online privacy suggests a functional mental model of online risks. However, since Cyberheroes was specifically tailored to younger children and Secure Comics was designed for a general audience including older children, we observed some differences, as well as several similarities, between the two studies.

9.3.1 The Elaboration Likelihood of Interactive Visual Narratives

The Elaboration Likelihood Model (ELM) [129] is traditionally used to explain persuasion through the central or peripheral routes to decision making. The central route requires motivated efforts to think logically and consciously about the message, potentially leading to a permanent change in attitude or behaviour. The peripheral route is mediated by superficial characteristics of the message presentation, potentially leading to a temporary change in attitude or behaviour. Research suggests that absorption from a narrative enhances the elaboration likelihood and persuasive effects [162]. In essence, comics and interactive ebooks are forms of narrative persuasion. Stories act as persuasive influence in many domains such as health communications [70] and entertainment-education [162].

Our work indeed found differences between interactive visual narratives and text-based narratives in their elaboration likelihood for children. Our study showed that interactive visual narratives had superior immediate and 1-week effects on children's privacy knowledge and behaviour than text narratives. After one week, the *comic* group in the Secure Comics study and the *ebook* group in the Cyberheroes study maintained the learned knowledge and behaviour while the *text* group from both studies showed a decrease in desired behaviour, suggesting that the comic was more successful at sustaining children's security motion after one week. Children who read visual interactive narratives demonstrated careful, logical, and conscious thinking about different scenarios in the post- and 1-week-tests and acted in a privacy-preserving manner on both occasions. This suggests that visual interactive narratives led to sustained changes in behaviour after one week and had a higher elaboration likelihood than the text-only narratives.

9.3.2 Knowledge Acquisition, Retention, and Transfer

Schmidt and Bjork [151] describe knowledge acquisition, retention, and transfer as the three phases of learning. *Knowledge acquisition* determines how well the learner can process and extract knowledge. In our study, children in both our conditions acquired knowledge and significantly improved their privacy knowledge post-reading.

Knowledge retention measures learners' ability to retain and recall information after some time. Children who viewed Cyberheroes and Secure Comics scored higher on privacy knowledge and behaviour tests after one week than those who read text-only narratives, demonstrating that interactive narratives assisted in knowledge retention. Cyberheroes included minimum text, lots of images, sounds, and a high-degree of user interaction. Secure Comics included more balanced portions of text and images, and modest user interaction. Past work cautioned that some multimedia features could act as distractors [42] and hinder comprehension [66]. However, our results from the two studies were mainly positive, particularly in the Cyberheroes study where children spent more time with the interactive ebook than the text-narrative, suggesting increased engagement and interest.

Our results align with Paivio's dual coding theory [34], which states that the combination of related text and images enhance comprehension and increase long-term memory. Education literature also supports the theory that depicting the content of accompanying text facilitates the construction of a lasting mental model [75]. In the two studies, we observed that user interaction contributed to mental model building. For example, on "digital trail" screen in Cyberheroes (see Figure 8.4, C), children performed an interaction where he/she attempted to "erase" the digital trail with a giant eraser, which led to parent-child conversations such as, *"you can try to erase it but what happens? If we erase it is it still there?"* (P3-ebook); *"yes"* (C3-ebook). In another example from the Secure Comics study, children interacted with the short story, "A day in the life of Jane", to discover how the character's various daily activities could reveal sensitive information. Our studies lend evidence of the benefits of visuals and interaction to help build mental models.

Knowledge transfer is the learner's ability to apply acquired knowledge to a closely related context (near-transfer) and to different situations (far-transfer). Our assessment of children's responses to different scenarios from Cyberheroes and Secure Comics suggested interactive visual narratives better supported both near and far knowledge transfer than the *text* control conditions. For example, C9-ebook from the Cyberheroes study described personal information as *"stuff that you don't want to tell other people, like where you live, what your password is. . . "* When asked about what she would do if her best friend asked to borrow her password, she was able to explain why passwords should be kept private, therefore demonstrating near transfer of knowledge: *"I wouldn't give her my password, because she could tell other people my personal stuff."* Children also demonstrated far transfer of knowledge in their response to alternate scenarios in the 1-Week-Test. For example, C9-ebook was able to recognize cyberbullying in different contexts and realize that her response would still be applicable; she gave the same response (*"I wouldn't send a message back and* *tell mama and papa."*) when cyberbullying was aimed towards herself (Post-Test scenario) or towards another kid (1-Week-Test scenario). In the Secure Comics study, children also responded to scenarios, but on the subjects of geo-tagging and online tracking. They demonstrated an elevated level of understanding that is consistent with the Cyberheroes study. For example, when inquired about what they should do in a situation where a friend ask them to post a group picture on their social media account, children were able to explain what they would do and how the situation could affect their own and others' privacy.

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

9.3.3 Effect of Interactivity

We found an overall positive influence from the interactive components included in Cyberheroes and Secure Comics. Children from the Secure Comics study suggested the inclusion of more interactive features. We therefore implemented a high degree of interactivity in Cyberheroes. We found the interactive components increased children's engagement with the ebook itself, with participants spending more time actually reading and interacting with the ebook than the text-narrative. It also increased engagement between the child and their parent; we observed them spending more time having privacy-related conversations and expanding on the content of the story. And perhaps most importantly, these interactions led to increased knowledge retention and knowledge transfer. Feedback from children suggested that Cyberhero's tailored multimedia-enhanced interactive storytelling and colourful illustration style appealed more to children than Secure Comics' more mature theme, modest interactive support, and monochromatic comic style.

9.3.4 Leveraging Previous Knowledge

Privacy and security are complex and potentially abstract concepts. Prior work [6, 50, 71, 72, 178] suggests that adults have poor mental models of security. Camp [87] identified five conceptual models that may be appropriate for adult risk communication: *physical security*, *medical infections*, *criminal behaviour*, *warfare*, and *economic failure*. We explored the first three models in Secure Comics to represent various privacy and security concepts in our adult studies [189].

In our work on children's privacy models in Chapter 7, we found that children also exhibited poor mental models that were even less sophisticated than those of adults. Unlike adults who may use a variety of conceptual models for online privacy and security, children mainly relied on their experiences with physical privacy and safety to navigate online spaces [191]. We suggested that the concept of physical security could be an appropriate conceptual model for children.

In the design of Cyberheroes, we leveraged children's existing understanding of parallel concepts in the physical world to communicate online privacy risks, and found that children could easily relate to concepts of identity, physical privacy, and safety. For example, in Cyberheroes, passwords are used to protect a vault, a physical map is used to trace Bobby's location, and an eraser is used to delete digital information. By grounding explanations in concepts that are already understood, we can help children use their experience to reason about new online situations in ways that help rather than hinder, formation of adequate mental models.

9.3.5 Limitations

The Cyberheroes interactive ebook was created by researchers with design and illustration experience. Some limitations of our work include that the sample size is small and not geographically diverse, and that the long-term effects of learning are compared to a text-only format and limited to one week. We also could not control for variability of dynamics within our participating families. Future work could study the long-term effects of the education tool on children's privacy knowledge and behaviour, and how parents and children would interact with it at home. It would also be interesting to study the effects of the ebook compared to other media formats, and how such privacy education tool could be adapted into the classroom setting in early elementary years as a instructional tool for teachers.

9.4 Conclusion

The Cyberheroes interactive ebook design addressed the challenge of transforming essential privacy information into an engaging format that resonated with young children. We suggest that online privacy education efforts need take into consideration that parents are sensitive towards children's exposure to 'frightening' topics or educational material that is inappropriate for their age. We showed that one way to communicate to children about a potentially serious and abstract topic such as online privacy is to leverage previously understood concepts to construct adequate mental models that children could use to reason about new online situations.

The Cyberheroes interactive ebook showed superior 1-week learning effects compared to conventional narrative text reading. Furthermore, our assessment of children's responses to different scenarios in their privacy knowledge and behaviour tests suggest that the interactive ebook supported superior transfer of knowledge than the *text* control condition after one week. Based on the three phases of learning (i.e., *knowledge acquisition, retention, transfer* [151]), this study suggests that the interactive ebook format is equally effective as the text narrative in *knowledge acquisition*, but superior in assisting effective *knowledge retention* and *knowledge transfer*. The Cyberheroes interactive ebook supported frequent co-reading interactions, and both parents and children said that it was engaging, easy to use, and easy to learn. Furthermore, interactive ebooks are useful in fostering child-parent discussions about the content that could lead to extended learning.

Chapter 10

Discussion, Conclusions, and Future Work

In Chapters 3 and 4, we proposed the Behaviour Model of Privacy and Security (BMOPS), and introduced a set of design principles from persuasive technology and instructional design. We applied the majority of these principles in the design of two types of multimedia tools about privacy and security for children, an interactive comic and an interactive ebook, and evaluated them with families. In this chapter, we discuss our experiences with the principles and whether they were useful for designing educational tools. Additionally, we discuss the implications of adult involvement in children's privacy and security education, and children's motivation and mental models in the context of the BMOPS model.

10.1 Use of Design Principles

Persuasive technology and instructional design principles were applied in the design of Secure Comics and Cyberheroes. From the evaluation of these prototypes, we found the principles supported multimedia educational approaches in different ways.

10.1.1 Engagement

To activate users' interest and engagement in learning privacy and security information, we embedded learning within fun and interactive activities: reading a digital interactive comic book and an interactive ebook. The ICAP framework [25] for differentiating levels of cognitive engagement in learning identifies four behavioural modes of learning: interactive (I), constructive (C), active (A), and passive (P). The framework's hypothesis predicts that learning will increase as learners become more cognitively engaged with the learning material, from passive receiving, to active manipulating, to constructive generating, to interactive dialoguing [25]. In passive modes of engagement, learners receive the information from the instructional material without overtly doing anything else learning related. In active modes of engagement, learners partake in some form of overt motor action or physical manipulation. Constructive modes of engagement occurs when learners generate or produce activities or materials beyond what was provided in the learning material. Lastly, interactive modes of engagement operationalize constructive dialogues between participants.

In our research studies, children chose the mode of learning. Children showed a preference for reading the text-only control silently/aloud without doing anything else, thus passively receiving the information. For our prototypes, the majority of 7 to 9-year-old children from the Cyberheroes study preferred co-reading aloud, or being read to aloud by a parent. The majority of 11 to 13-year-old children from the Secure Comics study preferred reading silently and independently from their parents. Based on the classifications of modes of learning from the ICAP framework [25], Secure Comics supported passive and active learning, while Cyberheroes supported passive, active, constructive, and interactive learning. Active learning was achieved in both prototypes by physically manipulating the interactive features and navigating between screens (e.g., pressing the forward or backward button). Constructive learning was achieved in Cyberheroes though parental support. Since the young children preferred to involved parents in the learning process, parents were able to supplement the concepts in the ebook with their own knowledge and examples from prior experiences. This stimulated dialogue by discussing the concepts together and enabling children to ask parents questions.

We believe the main design principles that facilitated active, constructive, and interactive learning in our prototypes were *multimedia* and *narrative*. Both Secure Comics and Cyberheroes used juxtaposition of multimedia including images, text and interactive elements to create interest and engagement. Both works also presented privacy and security information in the context of a narrative. The story of Secure Comics was written with a general audience in mind. Feedback from children suggested additional character development and a more intriguing plot would be more engaging. In Cyberheroes, we created the story *tailored* specifically to children that included a more imaginative plot and a focus on character development. Educational messages in Cyberheroes were fully integrated into a tailored narrative, making the educational intent less obvious and obtrusive than other types of multimedia learning systems, such as learning modules. Feedback from children suggested that they found the tailored story highly appealing. Some children read Cyberheroes more than once, suggesting that it was an enjoyable experience. Principles that attributed social influence in the interface like *social cues* and *socialization* also contributed to user immersion in the material. We used of pedagogical agents in Secure Comics, and characters that are like our target age group in Cyberheroes that had friendly social attributes and spoke using casual language. Usability evaluations from children showed that these characteristics generated positive attitudes toward the characters. Children found Secure Comics and Cyberheroes fairly engaging and the majority of children would read them again.

Our experience with multimedia was mainly positive. However, researchers caution that using an excess of multimedia in educational material could distract learners from key instructional points, disrupt their ability to mentally organize information, and activate irrelevant prior knowledge that increases the cognitive load [48]. Therefore, designers of children's educational multimedia system should avoid the use of extraneous multimedia.

Engagement Conclusion: Ideally, multimedia should extend learning by providing meaningful juxtaposing of visual, textual, and auditory information. We suggest that unobtrusive educational messages that are fully integrated into a tailored narrative would more engaging for children than overt training, and that parents should be involved in younger children's multimedia learning to promote constructive and interactive learning.

10.1.2 Knowledge and Retention

Research suggests that when text is integrated on the screen close to related visuals, learning is more effective than when they are placed in isolation [106]. We applied the *contiguity* principle and used visuals to depict the content of accompanying text to facilitate comprehension and retention. This principle adheres to Paivio's dual coding theory [34], which suggests that graphics and text are coded into memory differently, and that the combination of related text and images helps to enhance comprehension, and increases long-term memory. The benefits of comics and illustrative interactive ebooks are that words and images are inherently contiguous. Additionally, design principles that reduce the cognitive load, including *reduction* and *segmenting* help to increase comprehension and memory.

The graphics in Secure Comics and Cyberheroes were designed to complement the text explanations to facilitate comprehension by illustrating connections between concepts or providing visual examples. Education theory suggests that depicting the content of accompanying text facilitates the construction of a mental model [75]. In our research studies, we observed that user interaction could help build mental models. For example, interaction that showed cause and effect relationships in Cyberheroes encouraged children to ask parents questions about the concepts, and led to frequent child-parent discussions during reading.

However, children's privacy tests showed no significant difference in their post-test privacy knowledge compared to the text-only control, showing that both the Secure Comics and Cyberheroes prototypes and text-only formats improved children's understanding of online privacy immediately after reading. One week later, however, both prototypes showed superior knowledge retention than the control, suggesting that the principles were effective for supporting memory in the longer term.

Knowledge and Retention Conclusion: Design principles that facilitates comprehension and reduces the cognitive load appear effective for increasing children's retention, and facilitating the construction of a more lasting mental model.

10.1.3 Behaviour

Our research studies showed that children's privacy behaviour in situational scenarios were significantly improved one week after viewing the prototypes, compared to the pre-test. Mixed results were found for the reported behavioural effects immediately after viewing the prototypes and the control; a significant difference in reported behaviour was found between the comic and text control for the 11 to 13-year-olds, but not between the ebook and the text control for the 7 to 9-year-olds. We speculate that this is because younger children needed more time to process the information, and that the interactive prototypes led to improved behaviour over time. Furthermore, behaviour may be related to the increased knowledge retention that our prototypes supported.

One our design strategies for Secure Comics and Cyberheroes was that once children understood what the risks were and why they should protect their online privacy, they would be in a better position to judge the tradeoffs in situations between the benefits of disclosing information (e.g., social connection) and the potential harm of disclosure. Since our prototypes improved children's information retention, they remembered the lessons learned and applied them to different scenarios one week later.

Interactive features in Secure Comics and Cyberheroes explored *procedural rhetoric* to persuade children toward a certain position. Both Secure Comics and Cyberheroes expressed a point of view that aimed to shape behaviour, and rhetoric was achieved through interaction with the story content. Both works fuse traditional narrative with interactive elements, and children interacted with the narrative pieces, prompting them to think about what is happening in the story. Our observations and audio recordings of child-parent reading sessions of our prototypes showed that interactive elements indeed prompted children to ponder about the narrative messages. This was particularly overt in child-parent discussions during co-reading of Cyberheroes. An example of discussion and interaction from one child-parent pair is provided in Section 9.2.2. Based on our observations and analysis of child-parent co-reading recordings, we believe that interaction with the story content increased the persuasive appeal of the messages, promoted critical-thinking, and contributed to children's overall improved behaviour.

Behaviour Conclusion: Our research suggests that improved knowledge and behaviour may be related. Therefore, we conclude that design principles that support knowledge acquisition and retention may also be useful to reinforce behaviour. Furthermore, principles that aim to persuade procedurally through user interaction are likely to improve children behaviour than no interaction.

10.1.4 Metaphors

Our interview study from Chapter 7 suggests that children relied on physical privacy and safety concepts to navigate online spaces [191]. Based on this finding, we designed Cyberheroes with concrete physical privacy metaphors to communicate abstract online privacy risks to children. Prior research of children and metaphors suggests that metaphor comprehension development is a continuous process that increases with age [127]. It is constrained primarily by limitations in children's knowledge and information processing abilities, and that the transfer of knowledge from one domain to another relies on the conceptual knowledge the child already has [174].

Metaphors used in Cyberheroes were pictorial and based on concepts that we thought would be familiar to children. For example, we portrayed the Internet as a city that children could go to; passwords protected a physical vault full of toys; and digital trails were illustrated as a maze that children could attempt to erase using an eraser. Textual information in Cyberheroes and the text-only condition contained no explicit metaphors.

Children's post-test results did not show superior comprehension for the interactive ebook with visual metaphors than the text-only condition. Although the interactive ebook enhanced children's recall one week later, we did not find clear evidence that metaphors contributed to the effect as children did not refer to the metaphors used in the interactive comic and ebook to help them explain privacy and security concepts during the post- and one-week tests. Conversely, we also did not find the metaphors hindered children's comprehension or retention.

Our design experience suggests that metaphors were most useful for pictorializing potentially abstract online concepts that have no obvious visual representations. Visualizing information makes the application of *multimedia* and *contiguity* principles possible, and has the potential to increase engagement in learning. Since online privacy and security concepts are usually abstract, it might be necessary to find ways to explain the concepts to children based on metaphors and apologies, because the literal representations are too technical and abstract for children to understand.

Metaphors Conclusion: We found metaphors useful for visualizing abstract concepts to children in pictorial format that enables the application of design principles like *multimedia* to increase engagement. Designers should be aware, however, that children may have difficulty interpreting metaphors that are not based on their existing conceptual knowledge, and that metaphors may not be more effective than other methods for improving children's retention and comprehension.

10.1.5 Usability

Several of the design principles supported children's developmental needs, such as their limited information processing abilities, attention, working memory abilities, and literacy [84]. Design principles that simplify the user interface like *reduction* and *segmenting* reduce visual complexity and enable children to focus on a few key items of interest. Secure Comics segmented information in chapters, sections, pages, and panels. For younger children, we reduced the information even more to single-page segments with minimum text. User interface components like navigation were also simplified for the younger children to increase usability. For example, we reduced navigation from the six-item text menu in Secure Comics to a collapsible three-item icon menu in Cyberheroes.

We created clear visual mappings (e.g., a pulsing circle in Secure Comics and a rotating star in Cyberheroes) to *signal* the interactive objects from the non-interactive. We found that children quickly learned what they could do with the symbols. Interestingly, the visual markers on top of the interactive elements conditioned children to seek them out in the interface. For example, children got increasingly more excited to "press the stars" in Cyberheroes as they progressed through the screens. Secure Comics and Cyberheroes also included a pulsing hand symbol to *signal* draggable objects. We noticed that children had some accuracy issues dragging objects to specific targets, but no difficulty with free dragging. For example, some difficulty was observed for dragging boxes to targets in Secure Comic's drag-and-drop mini quiz game, but not in Cyberheroes' drag-objects-anywhere interactions. Our observations suggest that single-touch gestures were more suitable for children's motor skills as they had an easier time using tap than drag gestures. However, drag gestures are suitable when dragging accuracy is not an issue.

Developmentally appropriate *immediate feedback* is needed to meet children's abilities and experience in understanding what is happening on the interface [84]. To maximize stimulation of children's senses, we included both visual feedback like images and animation, and auditory feedback like sound and voice effects. However, beyond the value of feedback to enable children to observe what is happening, we believe the *immediate feedback* principle also created opportunities for *reflection* and motivated parent-child discussions. Unlike the interactive comic and ebook, our text-only conditions did not have any feedback. Children and parents simply read the story. In contrast, the interactive comic and ebook could be read, heard, and looked at. Feedback after an action caused children to ask questions or comment on the changes that took place. For example, the visual and auditory feedback on the "chatting online" screen in Cyberheroes prompted children to inquire more about the identity of the onscreen characters and the issue of trust. We believe meaningful feedback in the interface was one of the main contributing factors that promoted frequent child-parent discussions during interaction with the Cyberheroes Interactive ebook. This feedback information was not available in the text-only version, where children simply read about what is happing in the scene.

Usability Conclusion: Design principles should support the usability of children's educational tools and meet children's developmental needs. Principles like *reduction* and *segmenting* account for children's limited information processing capabilities to allow them to focus on a few things at a time. Children's user interface should have clear affordances to *signal* the location of interactive elements, and tap gesture is preferred over drag gesture for selection. *Immediate feedback* is a useful principle in children's user interface for providing visual, textual, or auditory cues about what is happening on screen, but also valuable in promoting child-parent interaction and discussion.

10.2 Implications of Adult Involvement

Our research suggests that parents want to educate children about online risks, but they also want to shelter them from online negativity [191]. Parents had varying opinions about the appropriate age for accessing various types of online tools and services like social media, and were thus cautious about children's early exposure to these subjects.

Children's primary online activities are playing games, watching video clips, instant messaging, and doing school work [99, 143, 166]. Many children 7 to 11 years old do not manage their own online accounts, passwords, and online purchases (e.g., apps) [191]. Parents are thus involved in children's daily interaction with technology and share the responsibility for managing children's privacy and security [2].

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

Given the parental dependency we observed in younger children, we believe involving parents in the education process is essential for this age group. Cyberheroes introduced children to essential online privacy concepts at an elementary level and inspired them to ask parents for more information about what they read. This empowered parents to disclose more information about specific topics at a level that they deem relevant and appropriate for their child. However, parental involvement could lead to different learning outcomes for children depending on the experiences of parents and how much information they chose to teach children. Future work could study the variability of families' attitudes towards online privacy and how they affect children's privacy education. Generally though, privacy education designed for young children should gently introduce privacy and safety concepts without scaring them, and should avoid topics that are irrelevant for their age.

10.3 Implications of Developmental Stages on Children's Motivation and Mental Models

In Chapter 3, we proposed the Behaviour Model of Privacy and Security (BMOPS). The model asserts high user motivation and functional mental models as related behavioural determinants for making privacy and security decisions. Usable privacy and security literature (e.g., [1, 178, 182]) suggests that end-users typically have low motivation and poor mental models when managing privacy and security tasks. Similarity, our interviews with children from Chapter 7 suggested that children also possess these characteristics. Privacy motivation, however, was described in the BMOPS model as being more personal and individually founded than security. This suggests that privacy motivation is more complex than security and difficult to generalize in the BMOPS model. Motivation could vary from "low" to "high" between individuals determined by their different circumstances, attitudes, and goals. Furthermore, changes in children's cognitive development [132] during the various stages of their lives suggest that children's privacy and security needs/concerns change and evolve over time. For example, our research suggests that children in the concrete operational stage (ages 7-11) are more dependent on adults for help and guidance than older children. As children enter the formal operational years (ages 11-16), they develop strong ties and influence with their peers, and parental influence decreases in comparison [28]. This stage also marks the start of puberty that causes strong emotional changes in children [28]. Children's privacy preferences shift as social media use substantially rises after age 11 [166]. These changes in children suggest differences in privacy preferences between age groups, and children could make different privacy and security decisions given similar situations at different stages in their lives. In some cases, more privacy might be undesirable as children strive to express themselves online, resulting in low motivation in the BMOPS model.

We argue, however, that functional mental models are always desirable in any online situation. Children should understand the consequences of their actions, but may decide that less privacy is a desirable tradeoff for them in some situations. Children's cognitive developmental stages offer some guidelines on how children at various stages may excel or struggle at learning privacy and security concepts. Our work suggests that children in the concrete operational stage should be introduced to these concepts at a basic level based on their existing conceptualizations of physical privacy and security. Children learn offline concepts like “stranger-danger”, private spaces (e.g., kids’ rooms, washrooms), and locking doors at an early age. We suggest these existing experiences could be leveraged to help children grasp new online privacy and security concepts. However, we believe building children’s mental models in the concrete operational stage is an ongoing process that goes beyond any one educational tool can provide. Specifically, parents play an important role in filling in any gaps that children might have. Based on our experience designing and evaluating educational tools for children, we suggest children’s educational technology should support co-use with parents and stimulate ongoing conversations concerning online issues. That way, children could build on the basic lessons learned as they gain new online experiences. As children grow from the concrete to the formal operational stage, they would become more prepared to understand the causes and effects of their online bahaviour and make informed privacy and security decisions.

Swan [167] suggests that children’s education should include digital literacy around using digital tools, critical literacy around interpreting and assessing information, and content literacy relating to composing and developing content. Our educational material focuses primarily on critical literacy, recognizing that children at different operational stages of development will need different lessons.

The children in our Cyberheroes study are in the concrete operational stage of development. This impacted the content of the lessons we selected for Cyberheroes, since we wanted to present the material in a manner accessible to this age group. For example, children of this age may focus on superficial markers of credibility and may have difficulty recognizing deception online [52,81,180]. Our educational material introduces the idea that not everyone (and everything) is as they seem and encourages children to turn to their parents for assistance. The goal is not necessarily to enable children to make these complex determinations, but to have them recognize that this is something requiring adult assistance and starting to prepare them for later lessons as they get older. As children gain more exposure and experience, they start to develop increasingly sophisticated decision-making strategies thus exposure to these concepts is beneficial to their development of secure and privacy-aware strategies. The children from the Secure Comics study have reached the formal operational stage of development and are thus more prepared for such credibility decisions [52].

The Limited Capacity Model (LCM) [95] discusses how children develop cognitively and how they perceive, store, and access information. Younger children have a less developed capacity and thus need information presented more simply than older children who have had opportunity to further develop their cognitive capacity. Earlier research suggested that children may have difficulty managing the complexities of assessing web content which may come from multiple sources and need to be attended to and evaluated separately [52]. However, with increased exposure to digital media (e.g., from infancy), it has been suggested that children may be developing the cognitive abilities to deal with such informational complexity at an earlier age [52]. Given this, gently introducing children to concepts of online privacy and security at a relatively young age is reasonable, and may help them to develop the cognitive abilities required to handle these complex issues at an earlier age than was previously expected.

In line with Mathieson [103], we believe that children should be given opportunities to develop the critical thinking skills and experience required to be aware and responsible digital citizens. Parental monitoring has its place and the degree of responsibility accorded to children will vary depending on the developmental stage of each individual child. The public also have different perceptions of what information should be shared. Notions of privacy, in particular, are constantly re-assessed by individuals to accommodate their changing circumstances, attitudes, and goals, making it difficult for educators to teach children exactly what information they should reveal and conceal. Therefore, we believe it is important to teach children critical thinking skills for assessing online situations and learning appropriate actions for their given circumstances, and to encourage ongoing conversation with adults. We feel that our empirically-tested Cyberheroes and Secure Comics are useful educational resources to aid in this process.

10.4 Future Work

To the best of our knowledge, this thesis is the first research-driven study on designing and evaluating privacy and security educational tools for younger children. The result of our studies inspired several future research directions.

Develop other multimedia approaches using a similar methodology: We explored two multimedia approaches in this thesis, an interactive comic and an interactive ebook. Since children responded positively to the superhero theme in Cyberheroes and found the connection between secret identities and online privacy easy to understand, our future work includes the development of a persuasive game based on our Cyberheroes interactive ebook. The game mechanic would explore the interplay between actions and consequences of children's privacy decisions. Games also enable the study of design principles that we were unable to explore in the interactive comic and ebook context, such the principles of simulation, monitoring, personalization, and rehearsal from persuasive technology. Using a similar methodology from our earlier work, the research would include design, development, and evaluation with families.

Study longer retention rates and behavioural effects: The maximum retention time and reported behavioural effects we studied in this thesis were one week. Future work could extend the work to study longer intervals of retention, such as at 3 or 6 months. Many families from our user studies expressed interest in using our other educational prototypes and asked for recommendations for privacy and security resources. Henceforth, it would worthwhile to followup whether the current prototypes inspired families to seek additional privacy and security training. Due to ethical concerns of putting children at risk, our measurement of children's behaviour was based on situational scenarios. A future extended study could investigate the prototypes' effects on children's privacy behaviour at home.

Extend the study in a classroom setting: Our prototypes have the potential to be incorporated into a school curriculum or course about online privacy and safety. A study could be conducted to compare the between-subject effects of a course integrated with and without the prototypes. It would be interesting to assess students' performances after using the prototype and whether the multimedia approach is more effective than traditional teaching approaches.

10.5 Thesis Summary

Online connectivity is an integral part of children's daily interaction with technology that increasingly exposes them to privacy and security risks. Computer security technology minimizes these risks, but their success is also dependent on individuals' behaviour that could be improved through education and training. Traditional computer privacy and security education work has success for adult users, but less is known of their effectiveness for children and how they can be appropriately designed to meet their specific developmental needs.

To address this gap in the research literature, we conducted empirical research to investigate the question, "Can multimedia approaches create effective, memorable, and persuasive tools for educating children about online privacy and security concepts?" We based our theoretical background on children's development literature, human factors in computer security, and established design principles from persuasive technology and instructional design. We explored how these can be successfully applied to the design children's educational tools for improving their privacy and security practices. We interviewed parents and children to understand prevalent mental models and perceived threat models. We designed Secure Comics and evaluated it with children 11 to 13 years old, and Cyberheroes with children 7 to 9 years old. Both studies showed superior improvements in children's privacy knowledge, retention, and privacy-conscious behaviour compared to text-only formats. We discussed our experiences using the design principles in our work and examined their usefulness in the increased knowledge and retention of content by children, and the usability of our prototypes.

10.6 Conclusion

Due to the limited empirical studies on the effectiveness of multimedia tools for educating children about privacy and security, our main goal in this research was to investigate the knowledge and behavioural learning effects of such tools. We focused our research on younger children, and successfully designed engaging interactive educational materials that improved their knowledge retention and prolonged the behavioural effects compared to text-only material. This empirical work suggests that persuasive technology and instructional design principles incorporated in multimedia materials increase engagement and improve the learning outcomes of educational content. Therefore, we conclude that multimedia tools are an effective approach for children's privacy and security education. Specifically, they improve children's knowledge retention and have the potential to influence children's behaviour in the longer term. However, we emphasize the need to adapt the design principles to address children's cognitive developmental needs. Furthermore, we suggest that children's privacy and security educational materials need to take into consideration families' learning preferences and various tolerance levels for exposing children to serious topics at a young age.

Bibliography

[1] A. Adams and M. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):41–46, 1999.

[2] T. Ammari, P. Kumar, C. Lampe, and S. Schoenebeck. Managing children's online identities: How parents decide what to disclose about their children online. *SIGCHI Conference on Human Factors in Computing Systems*, 2015.

[3] C. L. Anderson and R. Agarwal. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613–643, 2010.

[4] J. R. Anderson, A. T. Corbett, K. R. Koedinger, and R. Pelletier. Cognitive tutors: Lessons learned. *Journal of Learning Sciences*, 4(2):167–207, 1995.

[5] Anti-Phishing Working Group. APWG CMU-Cylab phishing education landing page program, Accessed June 2013. `http://phish-education.apwg.org`.

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

[7] R. K. Atkinson. Optimizing learning from examples using animated pedagogical agents. *Journal of Educational Psychology*, 94(2):416, 2002.

[8] A. D. Baddeley and G. Hitch. Working memory. *Psychology of learning and motivation*, 8:47–89, 1974.

[9] R. Balebako, J. Jung, W. Lu, L. Cranor, and C. Nguyen. Little brothers watching you: Raising awareness of data leaks on smartphones. In *Symposium on Usable Privacy and Security (SOUPS)*, 2013.

[10] D. E. Bambauer. Privacy versus security. *J. Crim. L. & Criminology*, 103:667, 2013.

[11] C. Bard, L. Hay, and M. Fleury. Timing and accuracy of visually directed movements in children: Control of direction and amplitude components. *Journal of Experimental Child Psychology*, 50(1):102–118, 1990.

[12] Barnard-Wills, David. Privacy Game, Accessed November 2016. `http://surveillantidentity.blogspot.ca/p/privacy-card-game.html`.

[13] M. Baslyman and S. Chiasson. "Smells phishy?": An educational game about online phishing scams. In *APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–11. IEEE, 2016.

[14] I. R. Berson and M. J. Berson. Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education*, 21(1):135–147, 2006.

[15] I. Bogost. *Persuasive games: The expressive power of videogames.* MIT Press, 2007.

[16] M. Borgi, I. Cogliati-Dezza, V. Brelsford, K. Meints, and F. Cirulli. Baby schema in human and animal faces induces cuteness perception and gaze allocation in children. *Frontiers in Psychology*, 5:411, 2014.

[17] C. J. Boyatzis and R. Varghese. Children's emotional associations with colors. *Journal of Genetic Psychology*, 155(1):77–85, 1994.

[18] R. K. Branson, G. T. Rayner, J. Cox, J. P. Furman, and F. J. King. Interservice procedures for instructional systems development: Executive summary and model. Technical report, DTIC Document, 1975.

[19] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[20] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. 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*, page 6. ACM, 2013.

[21] J. Burkell and A. Fortier. Privacy and control in online social profiles: Toward a typology of users. *American Society for Information Science and Technology*, 51(1):1–4, 2014.

[22] J. Burkell, A. Fortier, L. L. Y. C. Wong, and J. L. Simpson. Facebook: Public space, or private space? *Information, Communication & Society*, 17(8):974–985, 2014.

[23] S. K. Card, J. D. Mackinlay, and B. Shneiderman. *Readings in information visualization: Using vision to think.* Morgan Kaufmann Pub, 1999.

[24] Y. Chen, K. Ramamurthy, and K.-W. Wen. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3):157–188, 2012.

[25] M. T. Chi and R. Wylie. The ICAP framework: Linking cognitive engagement to active learning outcomes. *Educational Psychologist*, 49(4):219–243, 2014.

[26] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot. Influencing users towards better passwords: Persuasive Cued Click-Points. In *British Computer Society: Human Computer Interaction (BCS-HCI)*, pages 121–130, 2008.

[27] S. Chiasson and C. Gutwin. Design principles for children's software. *Computer Science Department, University of Saskatchewan*, 2005.

[28] S. Chiasson and C. Gutwin. Design principles for children's software. Technical Report HCI-TR-05-02, Computer Science Dept, University of Saskatchewan, 2005.

[29] S. Chiasson, M. Manas, and R. Biddle. Auction Hero: The design of a game to learn and teach about computer security, Accessed July 2013. `http://hotsoft.carleton.ca/~sonia/content/Chiasson_Auctionhero_ELearn2011.pdf`.

[30] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symp.*, pages 1–16, 2006.

[31] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, 2006.

[32] S. Chiasson, P. C. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*, pages 359–374. Springer, 2007.

[33] I. L. Child, J. A. Hansen, and F. W. Hornbeck. Age and sex differences in children's color preferences. *Child Development*, pages 237–247, 1968.

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

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

[36] R. C. Clark. *Developing technical training: A structured approach for developing classroom and computer-based instructional materials.* John Wiley & Sons, 2011.

[37] W. Commons. ADDIE model of design, Accessed July 2013. `http://upload.wikimedia.org/wikipedia/commons/d/d3/ADDIE_Model_of_Design.jpg`.

[38] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen. A video game for cyber security training and awareness. *Computers & Security*, 26(1):63–72, 2007.

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

[40] R. G. d'Andrade. *The development of cognitive anthropology.* Cambridge University Press, 1995.

[41] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

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

[43] J. S. DeLoache and C. M. Smith. Early symbolic representation. *Development of mental representation: Theories and applications*, pages 61–86, 1999.

[44] F. N. Dempster. Memory span: Sources of individual and developmental differences. *Psychological Bulletin*, 89(1):63, 1981.

[45] T. Denning, T. Kohno, and A. Shostack. Control-Alt-Hack: A card game for computer security outreach and education. In *ACM Technical Symposium on Computer Science Education*, pages 729–729. ACM, 2013.

[46] S. Deterding, D. Dixon, R. Khaled, and L. Nacke. From game design elements to gamefulness: Defining gamification. In *MindTrek conference: Envisioning future media environments*, pages 9–15. ACM, 2011.

[47] R. Dhamija and A. Perrig. Deja vu – a user study: Using images for authentication. In *USENIX Security Symposium*, volume 9, pages 4–4, 2000.

[48] N. M. Dixon. *Evaluation: A tool for improving HRD quality.* University Associates, San Diego, 1990.

[49] C. Dormann and R. Biddle. A review of humor for computer games: Play, laugh and more. *Simulation & gaming*, 40(6):802–824, 2009.

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

[51] A. Druin, B. B. Bederson, J. P. Hourcade, L. Sherman, G. Revelle, M. Platner, and S. Weng. Designing a digital library for young children. In *ACM/IEEE-CS Joint Conference on Digital libraries*, pages 398–405. ACM, 2001.

[52] M. S. Eastin, M.-S. Yang, and A. I. Nathanson. Children of the net: An empirical exploration into the evaluation of internet content. *Journal of Broadcasting & Electronic Media*, 50(2):211–230, 2006.

[53] S. Egelman and E. Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Human Factors in Computing Systems*, pages 2873–2882. ACM, 2015.

[54] S. Elo and H. Kyngäs. The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1):107–115, 2008.

[55] Federal Trade Commission (FTC). Children's Online Privacy Protection Act. http://www.coppa.org, 1998.

[56] R. Fivush, J. T. Gray, and F. A. Fromhoff. Two-year-old talk about the past. *Cognitive Development*, 2(4):393–409, 1987.

[57] J. H. Flavell, P. H. Miller, and S. A. Miller. *Cognitive development.* Prentice-Hall, Inc, 1993.

[58] B. J. Fogg. *Persuasive technology: Using computers to change what we think and do.* Morgan Kaufmann, San Francisco, 2003.

[59] B. J. Fogg. A behavior model for persuasive design. In *Persuasive Technology*, page 40. ACM, 2009.

[60] W. Ford. *Computer communications security: Principles, standard protocols and techniques.* Prentice-Hall, Inc., 1994.

[61] G. Freytag. *Freytag's technique of the drama: An exposition of dramatic composition and art.* Scholarly Press, 1896.

[62] S. Furnell, P. Bryant, and A. D. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410–417, 2007.

[63] R. M. Gagne, W. W. Wager, K. C. Golas, J. M. Keller, and J. D. Russell. *Principles of instructional design.* Wiley Online Library, 2005.

[64] GameSalad Inc. Gamesalad, Accessed February 2017. https://gamesalad.com.

[65] V. Garg and L. Camp. Risk characteristics, mental models, and perception of security risks. 2015.

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

[67] J. P. Gee. What video games have to teach us about learning and literacy. *Computers in Entertainment (CIE)*, 1(1):20–20, 2003.

[68] S. Gilutz and J. Nielsen. *Usability of websites for children: 70 design guidelines.* NN/g, Nielsen Norman Group, 2002.

[69] M. Gondree and Z. N. Peterson. Valuing security by getting [d0x3d!]. In *Workshop on Cyber Security Experimentation and Test, Washington, DC*, 2013.

[70] M. J. Green, K. R. Myers, et al. Graphic medicine: Use of comics in medical education and patient care. *BMJ*, 340, 2010.

[71] R. E. Grinter, W. K. Edwards, M. W. Newman, and N. Ducheneaut. The work to make a home network work. In *Computer Supported Cooperative Work*, pages 469–488. Springer, 2005.

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

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

[74] K. L. Gustafson and R. M. Branch. What is instructional design. *Trends and Issues in Instructional Design and Technology*, pages 16–25, 2002.

[75] V. Gyselinck and H. Tardieu. The role of illustrations in text comprehension: What, when, for whom, and why? 1999.

[76] S. F. Harp and R. E. Mayer. How seductive details do their damage: A theory of cognitive interest in science learning. *Journal of Educational Psychology*, 90(3):414, 1998.

[77] J. Hattie and H. Timperley. The power of feedback. *Review of Educational Research*, 77(1):81–112, 2007.

[78] R. J. Havighurst. Human development and education. 1953.

[79] T. Herath and H. R. Rao. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2):106–125, 2009.

[80] C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Workshop on New Security Paradigms Workshop (NSPW)*, pages 133–144. ACM, 2009.

[81] S. G. Hirsh. Children's relevance criteria and information seeking on electronic resources. *Journal of the Association for Information Science and Technology*, 50(14):1265, 1999.

[82] B. Hogan. The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, page 0270467610385893, 2010.

[83] C. J. Hoofnagle, J. King, S. Li, and J. Turow. How different are young adults from older adults when it comes to information privacy attitudes and policies? 2010.

[84] J. P. Hourcade. Child-computer interaction. *Self*, 2015.

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

[86] J. Paul Getty Trust. Principles of design, Accessed February 2011. `http://www.getty.edu/education/teachers/building_lessons/principles_design.pdf`.

[87] C. Jean. Mental models of privacy and security. *IEEE Tech. and Society*, 28(3), 2009.

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

[89] J. Kaye. Self-reported password sharing strategies. In *Human Factors in Computing Systems*, pages 2619–2622. ACM, 2011.

[90] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A nutrition label for privacy. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009.

[91] B. Knijnenburg and D. Cherry. Comics as a medium for privacy notices. In *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

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

[93] K. Krippendorff. *Content analysis: An introduction to its methodology.* Sage Publications, 1980.

[94] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J. Hong. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *APWG eCrime Summit*, pages 70–81. ACM, 2007.

[95] A. Lang. The limited capacity model of mediated message processing. *Journal of Communication*, 50(1):46–70, 2000.

[96] R. LaRose, N. J. Rifon, and R. Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, 2008.

[97] A. Lenhart, M. Madden, A. Smith, K. Purcell, K. Zickuhr, and L. Rainie. Teens, kindness and cruelty on social network sites: How American teens navigate the new world of digital citizenship. *Pew Internet & American Life Project*, 2011.

[98] S. Livingstone. Children's privacy online: Experimenting with boundaries within and beyond the family. *Computers, Phones, and the Internet: Domesticating Information Technology*, pages 128–144., 2011.

[99] S. Livingstone and M. Bober. Uk children go online: Surveying the experiences of young people and their parents. 2004.

[100] A. Marcus. Metaphor design for user interfaces. In *Human Factors in Computing Systems*, pages 129–130. ACM, 1998.

[101] G. Marx and V. Steeves. From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society*, 7(3/4):192–230, 2010.

[102] S. A. Mathan and K. R. Koedinger. Fostering the intelligent novice: Learning from errors with metacognitive tutoring. *Educational Psychologist*, 40(4):257–265, 2005.

[103] K. Mathiesen. The internet, children, and privacy: The case against parental monitoring. *Ethics and Information Technology*, 15(4):263–274, 2013.

[104] R. E. Mayer. Multimedia learning. *Psychology of Learning & Motivation*, 41:85–139, 2002.

[105] R. E. Mayer. Principles for reducing extraneous processing in multimedia learning: Coherence, signaling, redundancy, spatial contiguity, and temporal contiguity principles. *The Cambridge Handbook of Multimedia Learning*, pages 183–200, 2005.

[106] R. E. Mayer and R. B. Anderson. The instructive animation: Helping students build connections between words and pictures in multimedia learning. *Journal of Educational Psychology*, 84(4):444, 1992.

[107] R. E. Mayer and P. Chandler. When learning is just a click away: Does simple user interaction foster deeper understanding of multimedia messages? *Journal of Educational Psychology*, 93(2):390, 2001.

[108] R. E. Mayer, G. T. Dow, and S. Mayer. Multimedia learning in an interactive self-explaining environment: What works in the design of agent-based microworlds? *Journal of Educational Psychology*, 95(4):806, 2003.

[109] Media Smarts. Click if you agree, Accessed November 2016. `http://mediasmarts.ca/digital-media-literacy/educational-games/click-if-you-agree-grades-7-9`.

[110] Media Smarts. Co-Co's AdverSmarts: An interactive unit on food marketing on the web, Accessed November 2016. `http://mediasmarts.ca/game/co-cos-adversmarts-interactive-unit-food-marketing-web`.

[111] Media Smarts. Privacy pirates: An interactive unit on online privacy, Accessed November 2016. `http://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9`.

[112] Media Smarts. Privacy playground: The adventures of the three cyberpigs, Accessed November 2016. `http://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9`.

[113] C. Mekhail. "A day in the life of the Jos": The design of an educational game on privacy. Master's thesis, Carleton University, Ottawa, 2016.

[114] C. Mekhail, L. Zhang-Kennedy, and S. Chiasson. Visualizations to teach about mobile online privacy. In *Persuasive Technology, Adjunct Proceedings*. Springer, 2014.

[115] C. Mekhail, L. Zhang-Kennedy, and S. Chiasson. Visualizations to teach about mobile online privacy. In *Persuasive Technology*, pages 43–47, 2014.

[116] M. Metzger, A. Flanagin, and E. Nekmat. Comparative optimism in online credibility evaluation among parents and children. *Journal of Broadcasting & Electronic Media*, 59(3):509–529, 2015.

[117] M. J. Metzger and A. J. Flanagin. *Digital media, youth, and credibility.* MIT press, 2008.

[118] G. A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological review*, 63(2):81, 1956.

[119] M. Z. Mintzer and J. G. Snodgrass. The picture superiority effect: Support for the distinctiveness model. *The American Journal of Psychology*, 112(1):113–146, 1999.

[120] J. A. Moon. *Reflection in learning and professional development: Theory and practice.* Routledge, 2013.

[121] R. Moreno, M. Reislein, and G. Ozogul. Using virtual peers to guide visual attention during learning. *Journal of Media Psychology: Theories, Methods, and Applications*, 22(2):52–60, 2010.

[122] K. Müller and V. Hömberg. Development of speed of repetitive movements in children is determined by structural changes in corticospinal efferents. *Neuroscience Letters*, 144(1):57–60, 1992.

[123] A. Negrete and C. Lartigue. Learning from education to communicate science as a good story. *Endeavour*, 28(3):120–124, 2004.

[124] J. Nielsen. User education is not the answer to security problems. *Alertbox*, 2004.

[125] A. Nijholt. Embodied agents: A new impetus to humor research. In *The April Fools' Day Workshop on Computational Humour*, volume 20. University of Twente, 2002.

[126] H. Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[127] D. R. Pawlowski, D. M. Badzinski, and N. Mitchell. Effects of metaphors on children's comprehension and perception of print advertisements. *Journal of Advertising*, 27(2):83–98, 1998.

[128] J. W. Pellegrino, J. D. Bransford, and M. S. Donovan. *How people learn: Bridging research and practice.* National Academies Press, 1999.

[129] R. E. Petty and P. Briñol. The elaboration likelihood model. *Handbook of theories of social psychology*, 1:224–245, 2011.

[130] J. Piaget. Logic and psychology. 1957.

[131] J. Piaget. *The language and thought of the child*, volume 5. Psychology Press, 1959.

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

[133] J. Piaget and B. Inhelder. *The psychology of the child.* Basic books, 2008.

[134] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. In *Symposium on Usable Privacy and Security (SOUPS)*, page 6. ACM, 2012.

[135] F. Raja, K. Hawkey, S. Hsu, K. Wang, and K. Beznosov. A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings. In *Symposium on Usable Privacy and Security (SOUPS).* ACM, 2011.

[136] J. R. Rausch, S. E. Maxwell, and K. Kelley. Analytic methods for questions pertaining to a randomized pretest, posttest, follow-up design. *Journal of Clinical Child and Adolescent Psychology*, 32(3):467–486, 2003.

[137] K. Raynes-Goldie and M. Allen. Gaming privacy: A canadian case study of a co-created privacy literacy game for children. *Surveillance & Society*, 12(3):414, 2014.

[138] J. C. Read and M. M. Bekker. The nature of child computer interaction. In *BCS conference on human-computer interaction*, pages 163–170. British Computer Society, 2011.

[139] J. C. Read and S. MacFarlane. Using the fun toolkit and other survey methods to gather opinions in child computer interaction. In *Interaction Design and Children (IDC)*, pages 81–88. ACM, 2006.

[140] B. Reeves and C. Nass. *How people treat computers, television, and new media like real people and places.* CSLI Publications & Cambridge University Press, 1996.

[141] H.-S. Rhee, C. Kim, and Y. U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, 2009.

[142] Richtel, M. Young, in love and sharing everything, including a password, Accessed January 2016. `http://www.nytimes.com/2012/01/18/us/teenagers-sharing-passwords-as-show-of-affection.html`.

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

[144] U. Ritterfeld, M. Cody, and P. Vorderer. *Serious games: Mechanisms and effects.* Routledge, 2009.

[145] B. Rittle-Johnson and M. W. Alibali. Conceptual and procedural knowledge of mathematics: Does one lead to the other? *Journal of Educational Psychology*, 91(1):175, 1999.

[146] R. W. Rogers. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1):93–114, 1975.

[147] M. Roussou. Learning by doing and learning through play: An exploration of interactivity in virtual environments for children. *Computers in Entertainment (CIE)*, 2(1):10–10, 2004.

[148] J. G. Ruiz, M. J. Mintzer, and R. M. Leipzig. The impact of e-learning in medical education. *Academic medicine*, 81(3):207–212, 2006.

[149] M. A. Sasse and I. Flechais. Usable security: Why do we need it? How do we get it? 2005.

[150] S. Schechter. The user is the enemy, and (s) he keeps reaching for that bright shiny power button. In *Workshop on Home Usable Privacy and Security (HUPS)*, 2013.

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

[152] J. Scott. Children as respondents: The challenge for quantitative methods. *Research With Children: Perspectives and Practices*, pages 98–119, 2000.

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

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

[155] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Symposium on Usable Privacy and Security (SOUPS)*, page 2. ACM, 2010.

[156] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 88–99. ACM, 2007.

[157] B. Shmueli and A. Blecher-Prigat. Privacy for children. *Columbia Human Rights Law Review*, 42:759–795, 2011.

[158] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[159] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: Implications for security design based on social practice. In *Human Factors in Computing Systems*, pages 895–904. ACM, 2007.

[160] A. Singhal and E. M. Rogers. *Entertainment-education: A communication strategy for social change*. Routledge, 2012.

[161] Six to Start. Smokescreen, Accessed November 2016. http://www.sixtostart.com/smokescreen/.

[162] M. D. Slater and D. Rouner. Entertainmenteducation and elaboration likelihood: Understanding the processing of narrative persuasion. *Communication Theory*, 12(2):173–191, 2002.

[163] M. Smarts. Canada's centre for digital and media literacy. http://mediasmarts.ca/, 2014.

[164] D. J. Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[165] S. Srikwan and M. Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, 2008.

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

[167] K. Swan. Nonprint media and technology literacy standards for assessing technology integration. *Journal of Educational Computing Research*, 23(1):85–100, 2000.

[168] **A. Forget**, S. Chiasson, R. Biddle, and P. C. van Oorschot. Persuasion as education for computer security. In *AACE E-Learn Conference*, pages 822–829, 2007.

[169] **A. Forget**, S. Chiasson, P. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *ACM Symposium on Usable Privacy and Security (SOUPS)*, pages 1–12, 2008. (28% accept rate).

[170] The Office of the Privacy Commissioner of Canada. Social Smarts: Privacy, the internet and you, Accessed September 2016. https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/social-smarts-privacy-the-internet-and-you/.

[171] E. Topolovac, M. Sammuli, and M. A. Smith. Checkpoints for progress in reading and writing for teachers and learning partners. 1997.

[172] J. Van der Pligt. Risk perception and self-protective behavior. *European Psychologist*, 1(1):34–43, 1996.

[173] J. R. Vickery. i don't have anything to hide, but': the challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, 18(3):281–294, 2015.

[174] S. Vosniadou. Children and metaphors. *Child Development*, pages 870–885, 1987.

[175] S. E. Wade. Research on importance and interest: Implications for curriculum development and future research. *Educational Psychology Review*, 13(3):243–261, 2001.

[176] S.-K. Wang and H.-Y. Hsu. Using the ADDIE model to design second life activities for online learners. *TechTrends*, 53(6):76–81, 2009.

[177] M. Warkentin, K. Davis, and E. Bekkering. Introducing the check-off password system (COPS): An advancement in user authentication methods and information security. *Organizational and End User Computing (JOEUC)*, 16(3):41–58, 2004.

[178] R. Wash. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010.

[179] R. Wash and E. Rader. Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 309–325, 2015.

[180] J. S. Watson. "if you don't have it, you can't find it." a close look at students' perceptions of using technology. *Journal of the American Society for Information Science*, 49(11):1024, 1998.

[181] A. F. Westin. Harris-equifax consumer privacy survey. *Atlanta, GA: Equifax Inc*, 1991.

[182] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security*, 1999.

[183] M. Williams, O. Jones, C. Fleuriot, and L. Wood. Children and emerging wireless technologies: Investigating the potential for spatial practice. In *SIGCHI Conference on Human Factors in Computing Systems*, pages 819–828. ACM, 2005.

[184] I. Woon, G.-W. Tan, and R. Low. A protection motivation theory approach to home wireless security. *International Conference on Information Systems (ICIS)*, page 31, 2005.

[185] G. Yang. Comics in education, Accessed September 2016. `http://www.humblecomics.com/comicsedu/index.html`.

[186] L. Zhang-Kennedy and S. Chiasson. Using comics to teach users about mobile online privacy. Technical Report TR-14-02, School of Computer Science, Carleton University, Ottawa, Canada, 2014.

[187] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *APWG eCrime Summit*. IEEE, 2013.

[188] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Stop clicking on 'update later': Persuading users they need up-to-date antivirus protection. In *Persuasive Technology*, pages 302–322. Springer LNCS, 2014.

[189] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, 2016.

[190] L. Zhang-Kennedy, E. Fares, S. Chiasson, and R. Biddle. Geo-phisher: The design and evaluation of information visualizations about internet phishing trends. In *APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–12. IEEE, 2016.

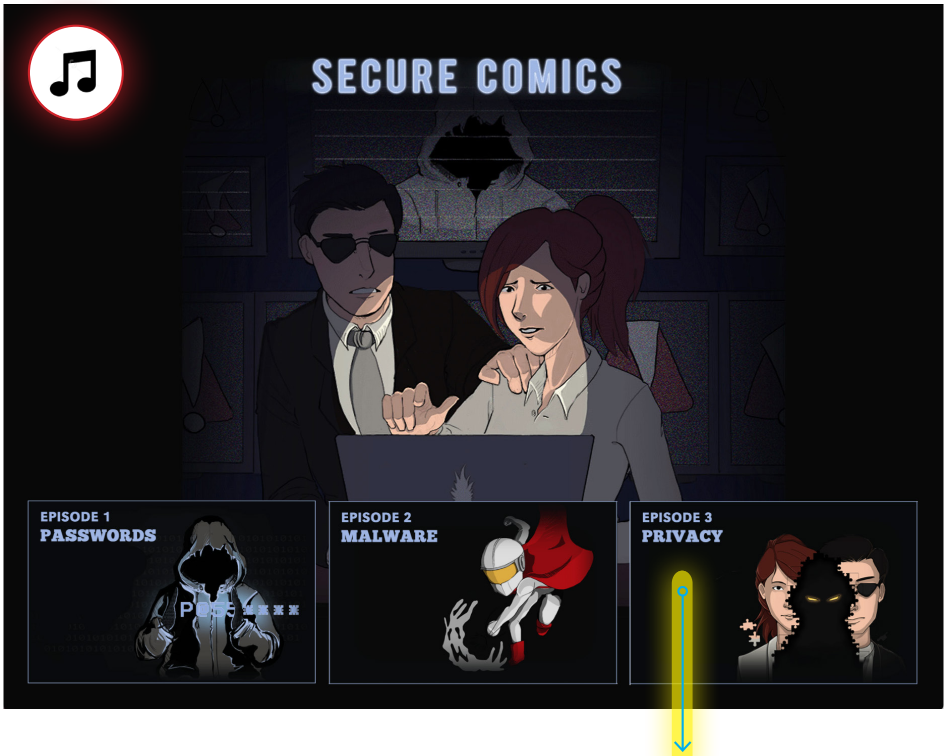
[191] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, and S. Chiasson. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Interaction Design and Children*, pages 388–399. ACM, 2016.

Appendix A

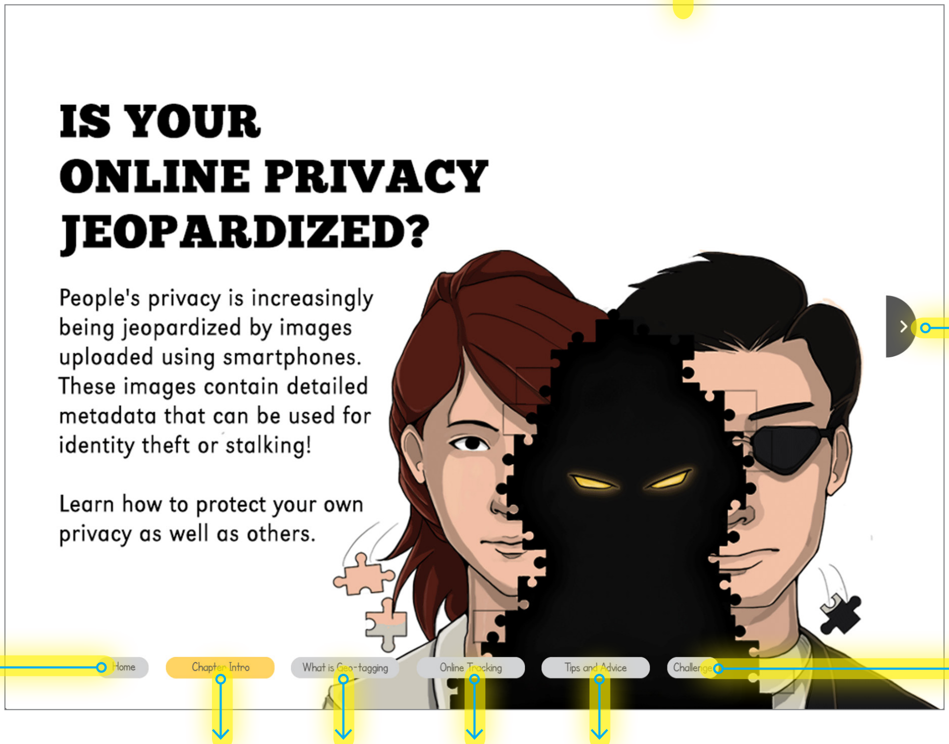
Secure Comics Design Documentation

Secure Comics About Mobile Online Privacy
Design Documentation

🔊	Sound Effect
🎬	Animation
♫	Backgound Music
○→	Navigation
○→	Interaction



Landing Screen



IS YOUR ONLINE PRIVACY JEOPARDIZED?

People's privacy is increasingly being jeopardized by images uploaded using smartphones. These images contain detailed metadata that can be used for identity theft or stalking!

Learn how to protect your own privacy as well as others.

Title Screen

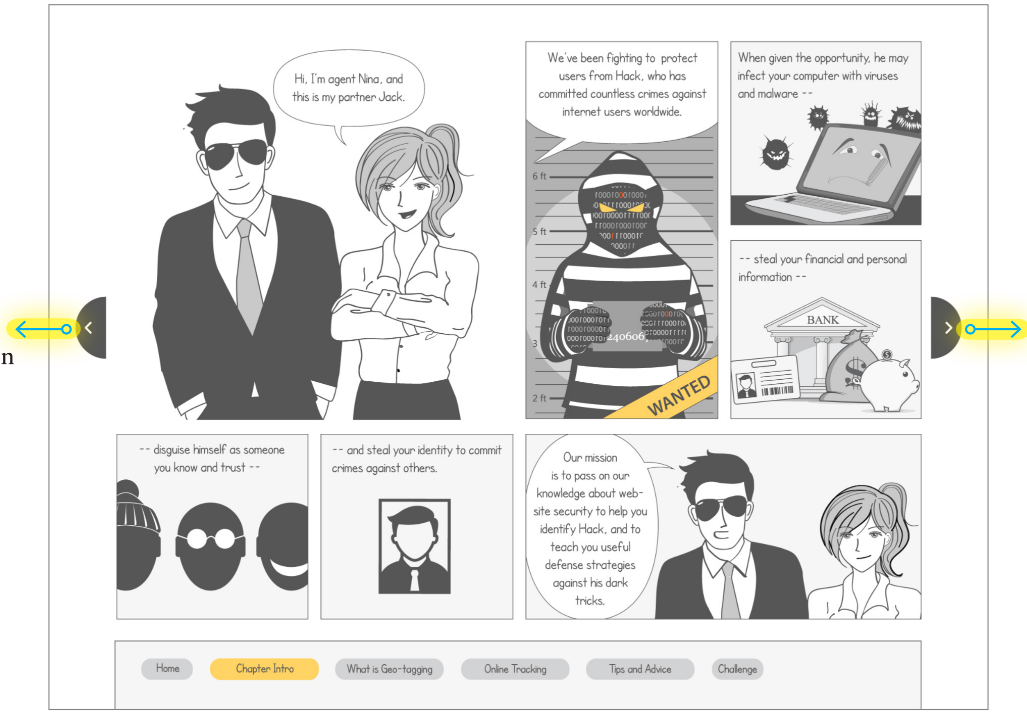
Pg. 1

Landing Screen

Pg. 9

Pg. 1 Pg. 2 Pg. 4 Pg. 6

Pg. 1



Hi, I'm agent Nina, and this is my partner Jack.

We've been fighting to protect users from Hack, who has committed countless crimes against internet users worldwide.

When given the opportunity, he may infect your computer with viruses and malware --

-- steal your financial and personal information --

-- disguise himself as someone you know and trust --

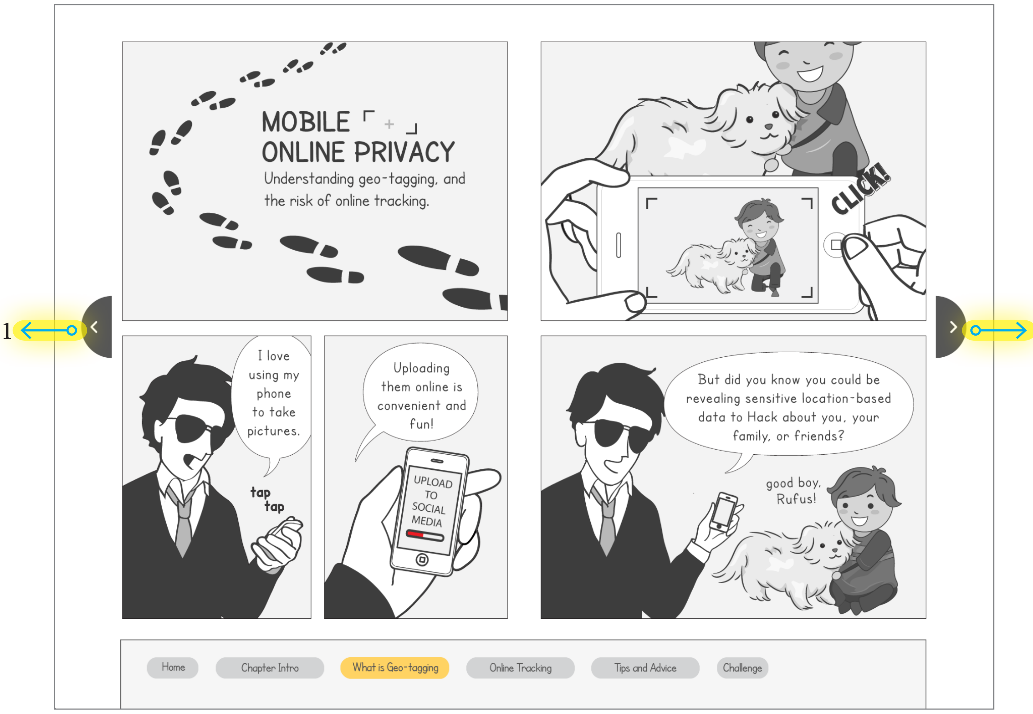
-- and steal your identity to commit crimes against others.

Our mission is to pass on our knowledge about website security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.

Title screen

Pg. 2

Pg. 2



MOBILE ONLINE PRIVACY

Understanding geo-tagging, and the risk of online tracking.

I love using my phone to take pictures.

Uploading them online is convenient and fun!

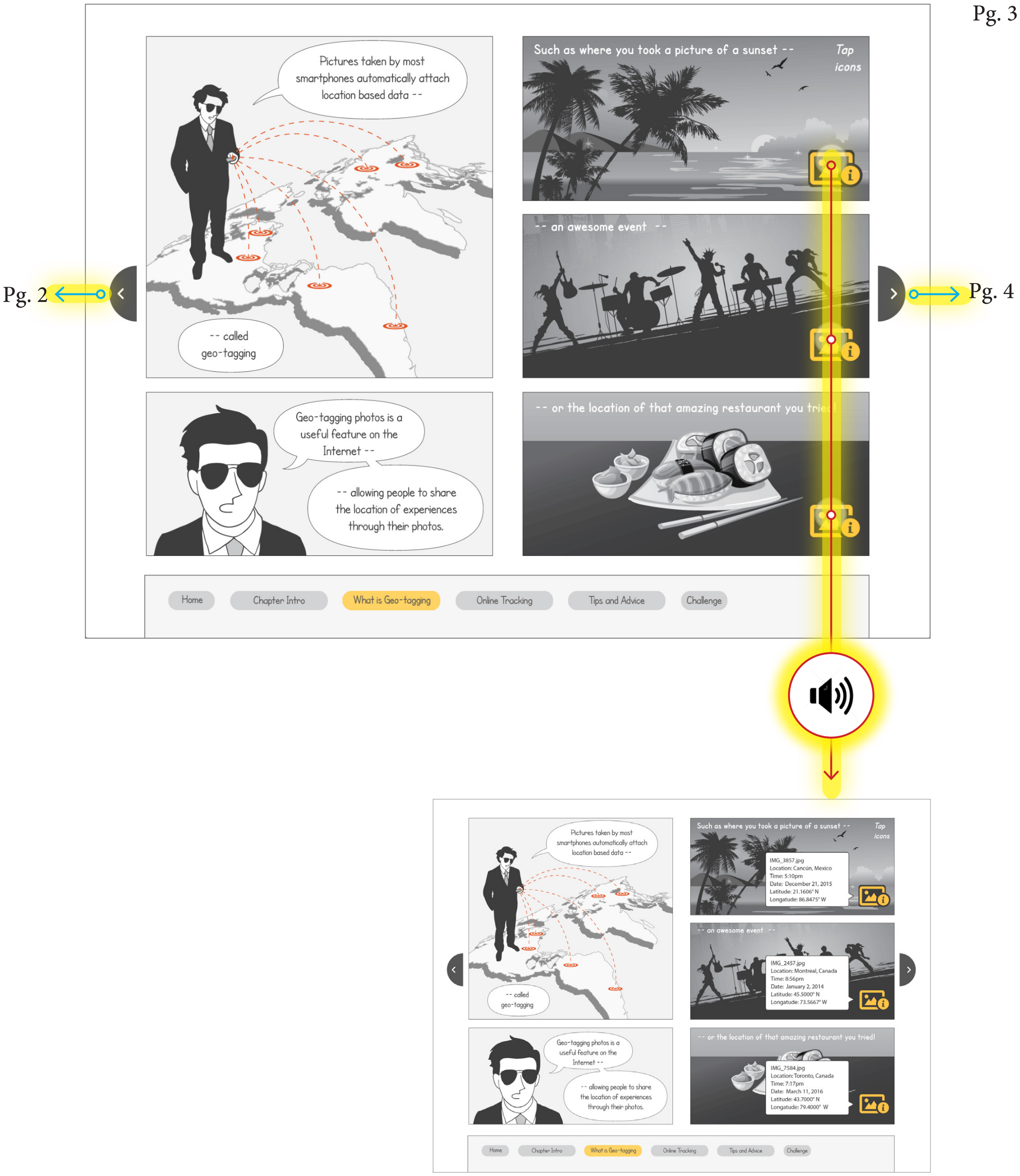
But did you know you could be revealing sensitive location-based data to Hack about you, your family, or friends?

good boy, Rufus!

Pg. 1

Pg. 3

Pg. 3


Pg. 2
Pg. 4
Pictures taken by most smartphones automatically attach location based data --
-- called geo-tagging
Geo-tagging photos is a useful feature on the Internet --
-- allowing people to share the location of experiences through their photos.
Such as where you took a picture of a sunset --
Tap icons
-- an awesome event --
-- or the location of that amazing restaurant you tried!
Home
Chapter Intro
What is Geo-tagging
Online Tracking
Tips and Advice
Challenge

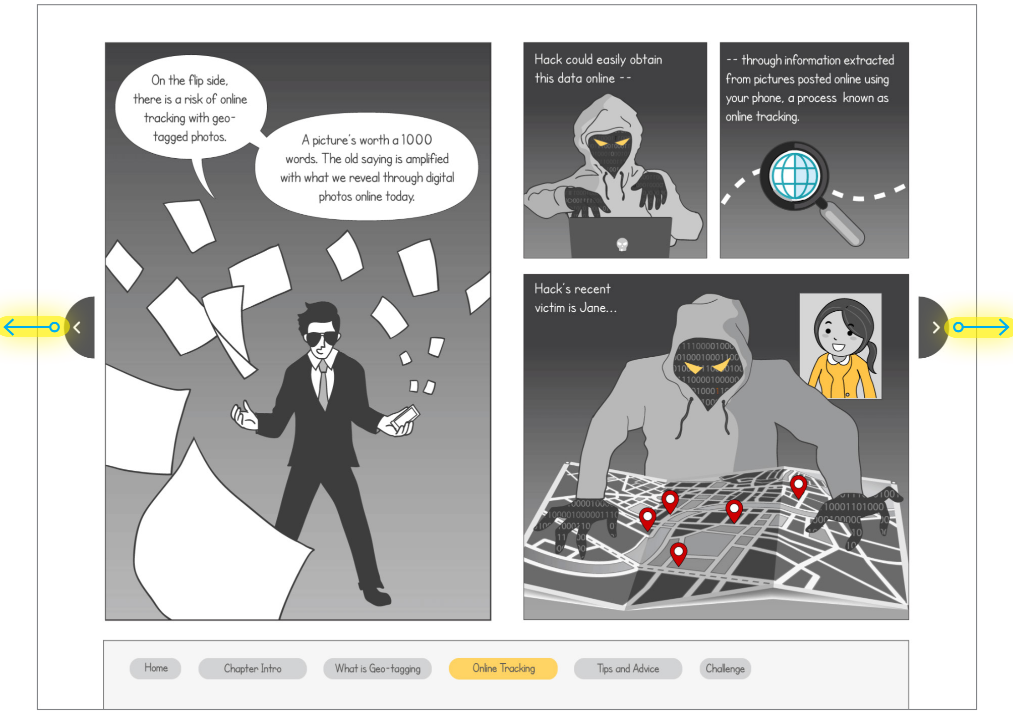
IMG_3857.jpg
Location: Cancún, Mexico
Time: 5:10pm
Date: December 21, 2015
Latitude: 21.1606° N
Longatude: 86.8475° W

IMG_2457.jpg
Location: Montreal, Canada
Time: 8:56pm
Date: January 2, 2014
Latitude: 45.5000° N
Longatude: 73.5667° W

IMG_7584.jpg
Location: Toronto, Canada
Time: 7:17pm
Date: March 11, 2016
Latitude: 43.7000° N
Longatude: 79.4000° W

Pg. 4

Pg. 3



On the flip side, there is a risk of online tracking with geo-tagged photos.

A picture's worth a 1000 words. The old saying is amplified with what we reveal through digital photos online today.

Hack could easily obtain this data online --

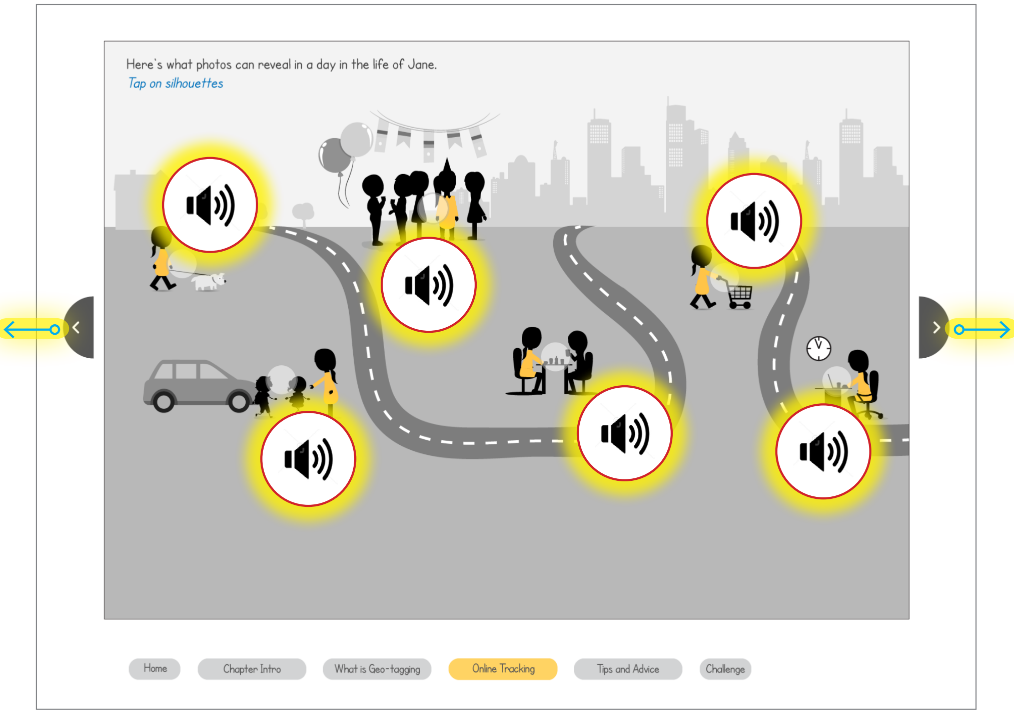
-- through information extracted from pictures posted online using your phone, a process known as online tracking.

Hack's recent victim is Jane...

Pg. 5

Pg. 5

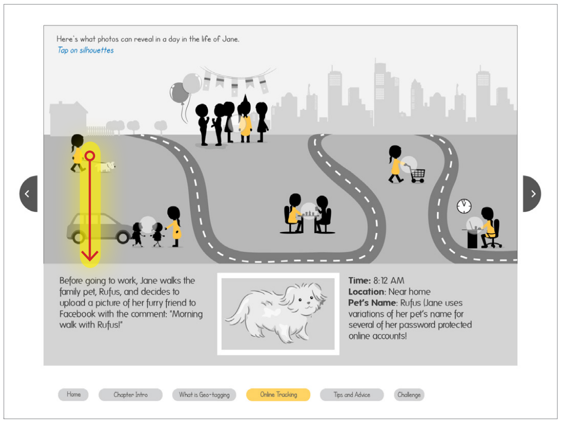
Pg. 4



Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

Pg. 6

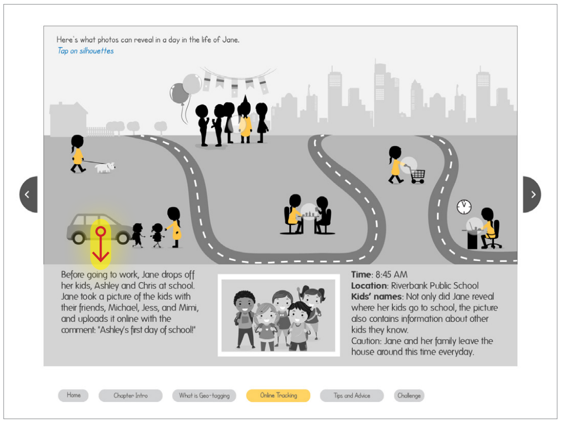


Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

Before going to work, Jane walks the family pet, Rufus, and decides to upload a picture of her furry friend to Facebook with the comment: "Morning walk with Rufus!"

Time: 8:12 AM
Location: Near home
Pet's Name: Rufus (Jane uses variations of her pet's name for several of her password protected online accounts!

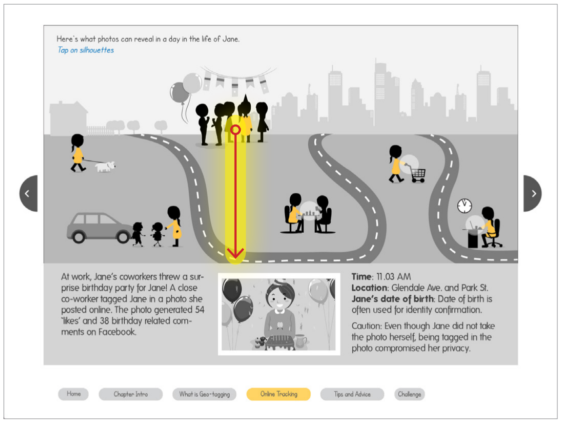


Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

Before going to work, Jane drops off her kids, Ashley and Chris at school. Jane took a picture of the kids with their friends, Michael, Jess, and Mimi, and uploads it online with the comment: "Ashley's first day of school!"

Time: 8:45 AM
Location: Riverbank Public School
Kids' names: Not only did Jane reveal where her kids go to school, the picture also contains information about other kids they know.
Caution: Jane and her family leave the house around this time everyday.



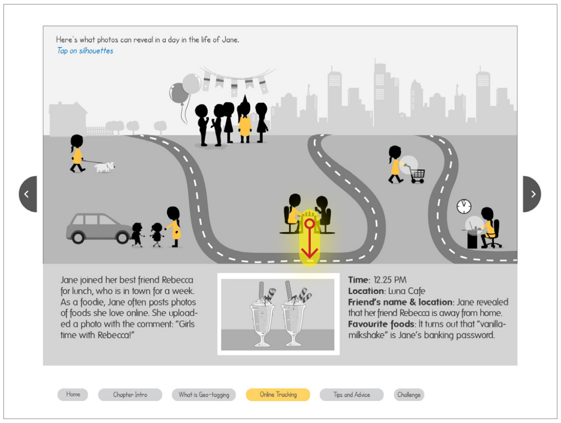
Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

At work, Jane's coworkers threw a surprise birthday party for Jane! A close co-worker tagged Jane in a photo she posted online. The photo generated 54 'likes' and 38 birthday related comments on Facebook.

Time: 11.03 AM
Location: Glendale Ave. and Park St.
Jane's date of birth: Date of birth is often used for identity confirmation.

Caution: Even though Jane did not take the photo herself, being tagged in the photo compromised her privacy.

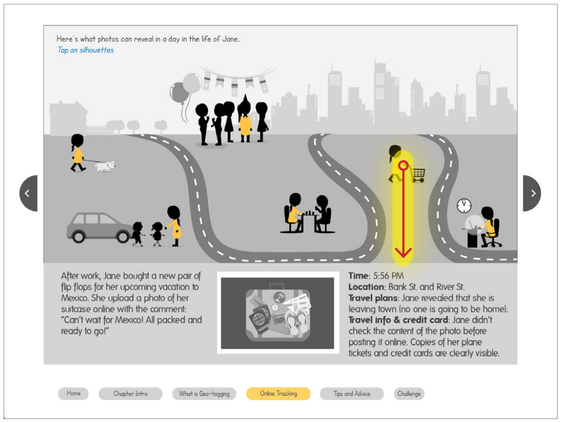


Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

Jane joined her best friend Rebecca for lunch, who is in town for a week. As a foodie, Jane often posts photos of foods she love online. She uploaded a photo with the comment: "Girls time with Rebecca!"

Time: 12.25 PM
Location: Luna Cafe
Friend's name & location: Jane revealed that her friend Rebecca is away from home.
Favourite foods: It turns out that "vanilla-milkshake" is Jane's banking password.

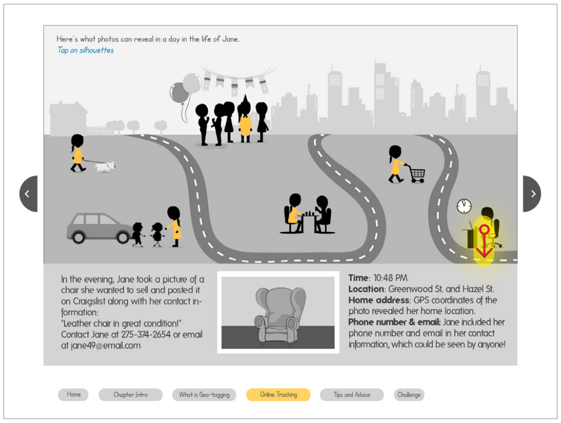


Here's what photos can reveal in a day in the life of Jane.

Tap on silhouettes

After work, Jane bought a new pair of flip flops for her upcoming vacation to Mexico. She upload a photo of her suitcase online with the comment: "Can't wait for Mexico! All packed and ready to go!"

Time: 5:56 PM
Location: Bank St. and River St.
Travel plans: Jane revealed that she is leaving town (no one is going to be home).
Travel info & credit card: Jane didn't check the content of the photo before posting it online. Copies of her plane tickets and credit cards are clearly visible.



Here's what photos can reveal in a day in the life of Jane.

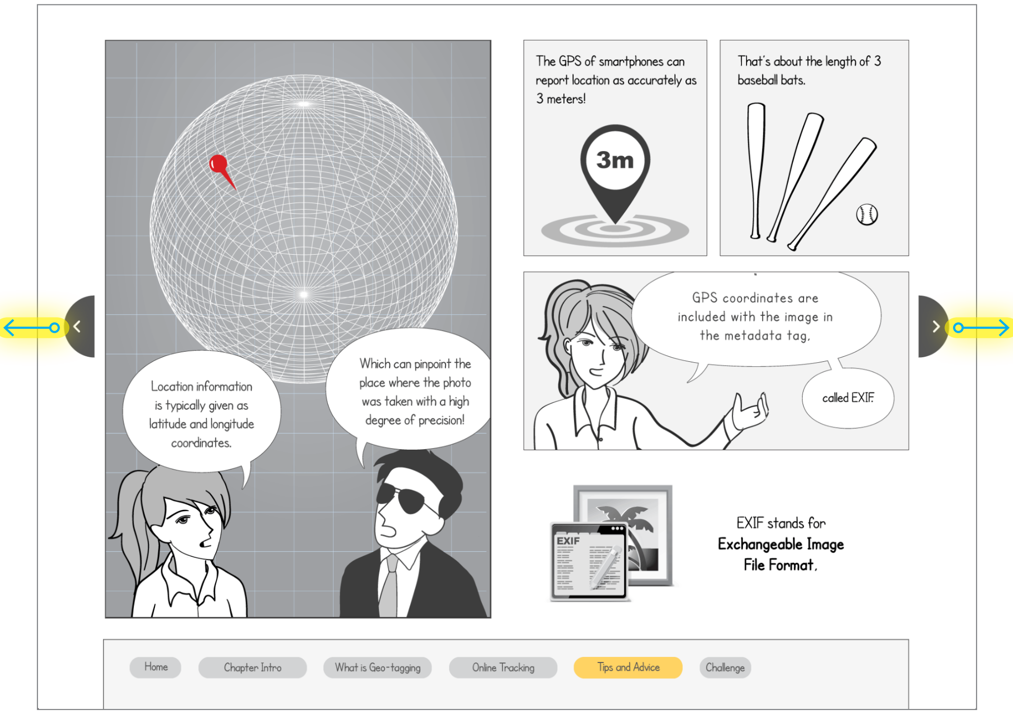
Tap on silhouettes

In the evening, Jane took a picture of a chair she wanted to sell and posted it on Craigslist along with her contact information:
"Leather chair in great condition!"
Contact Jane at 275-374-2654 or email at jane49@email.com

Time: 10:48 PM
Location: Greenwood St. and Hazel St.
Home address: GPS coordinates of the photo revealed her home location.
Phone number & email: Jane included her phone number and email in her contact information, which could be seen by anyone!

Pg. 6

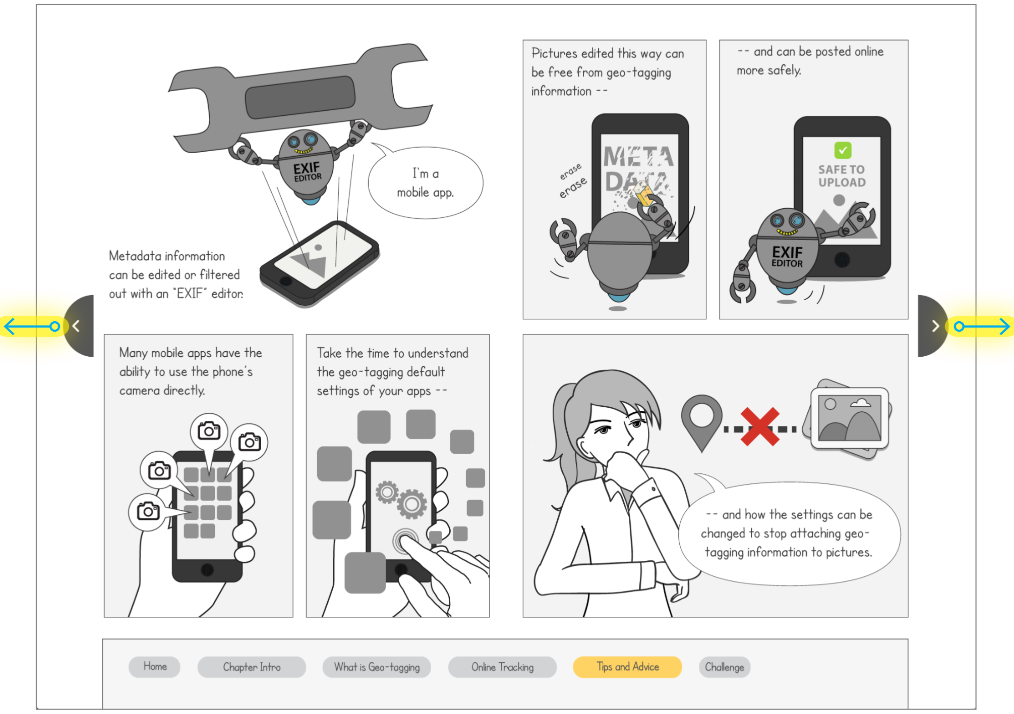
Pg. 5


Location information is typically given as latitude and longitude coordinates.
Which can pinpoint the place where the photo was taken with a high degree of precision!
The GPS of smartphones can report location as accurately as 3 meters!
3m
That's about the length of 3 baseball bats.
GPS coordinates are included with the image in the metadata tag,
called EXIF.
EXIF
EXIF stands for **Exchangeable Image File Format.**
Home
Chapter Intro
What is Geo-tagging
Online Tracking
Tips and Advice
Challenge

Pg. 7

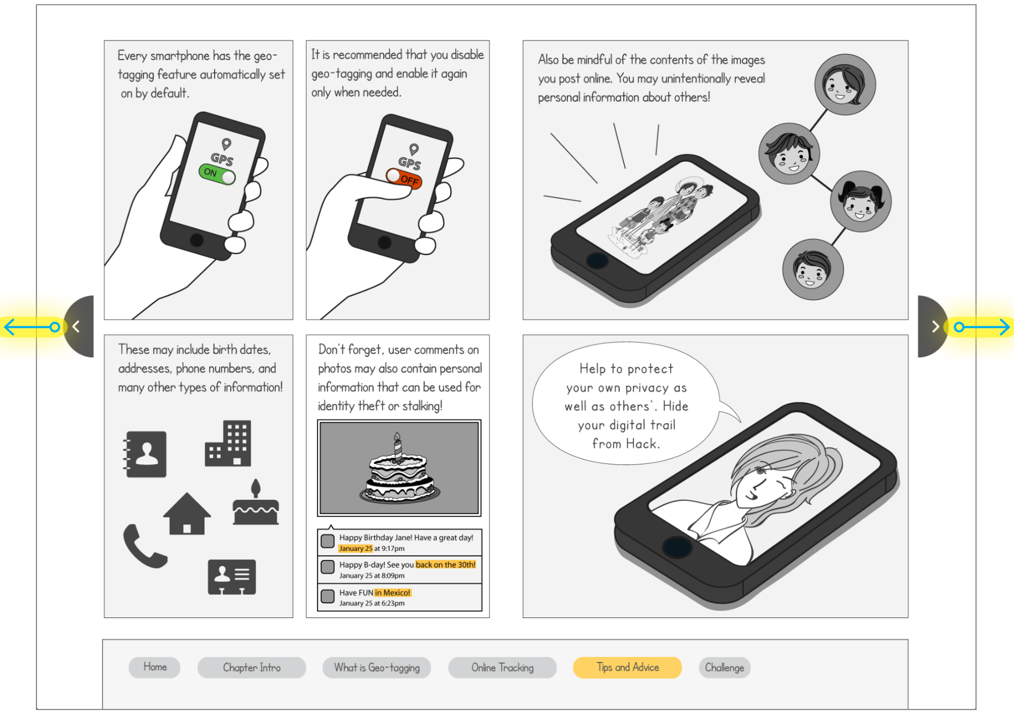
Pg. 7

Pg. 6


EXIF EDITOR
I'm a mobile app.
Metadata information can be edited or filtered out with an "EXIF" editor.
Pictures edited this way can be free from geo-tagging information --
erase erase
META DATA
-- and can be posted online more safely.
SAFE TO UPLOAD
EXIF EDITOR
Many mobile apps have the ability to use the phone's camera directly.
Take the time to understand the geo-tagging default settings of your apps --
-- and how the settings can be changed to stop attaching geo-tagging information to pictures.
Home
Chapter Intro
What is Geo-tagging
Online Tracking
Tips and Advice
Challenge

Pg. 8

Pg. 8



Every smartphone has the geo-tagging feature automatically set on by default.

It is recommended that you disable geo-tagging and enable it again only when needed.

Also be mindful of the contents of the images you post online. You may unintentionally reveal personal information about others!

These may include birth dates, addresses, phone numbers, and many other types of information!

Don't forget, user comments on photos may also contain personal information that can be used for identity theft or stalking!

Happy Birthday Jane! Have a great day!
January 25 at 9:17pm

Happy B-day! See you back on the 30th!
January 25 at 8:09pm

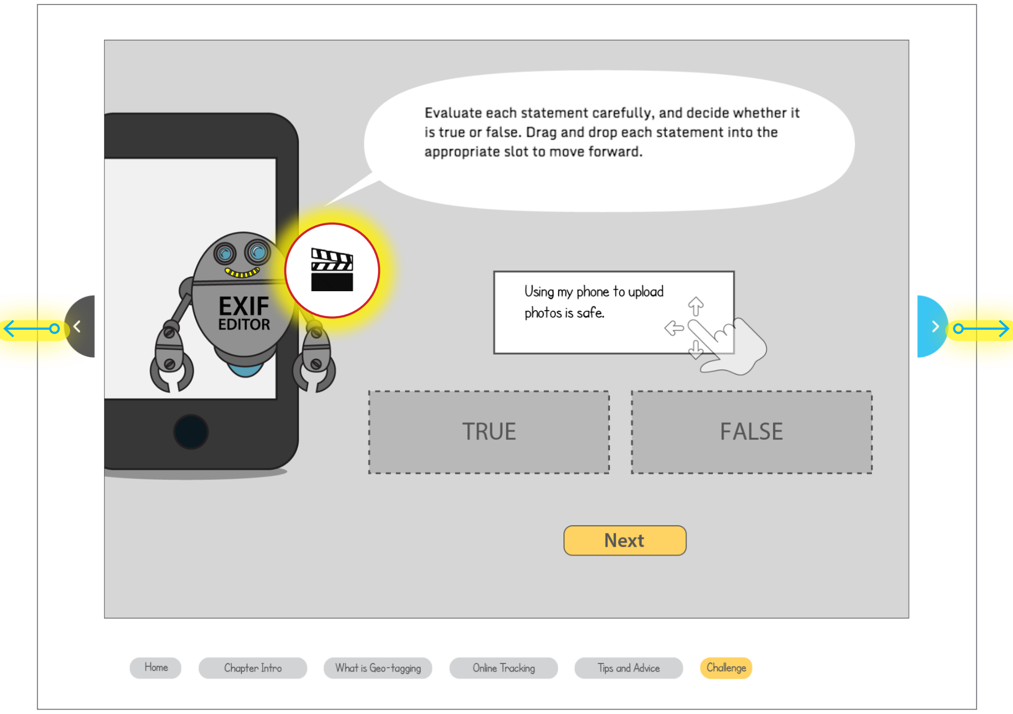
Have FUN in Mexico!
January 25 at 6:23pm

Help to protect your own privacy as well as others'. Hide your digital trail from Hack.

Pg. 7

Pg. 9

Pg. 9



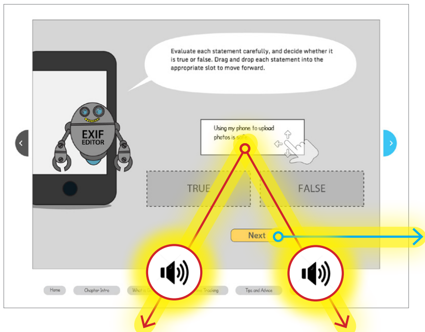
Evaluate each statement carefully, and decide whether it is true or false. Drag and drop each statement into the appropriate slot to move forward.

Using my phone to upload photos is safe.

Pg. 8

Next Chapter

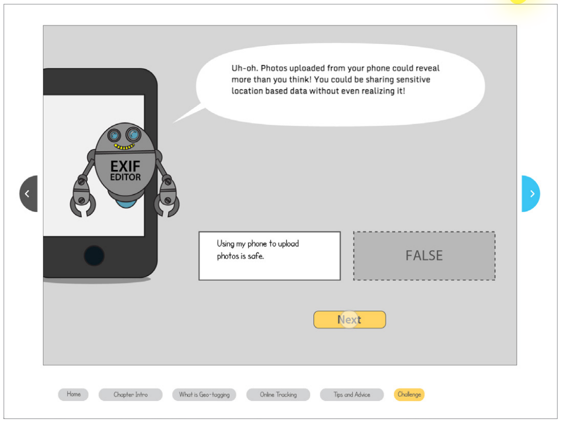
Q. 1



Evaluate each statement carefully, and decide whether it is true or false. Drag and drop each statement into the appropriate slot to move forward.

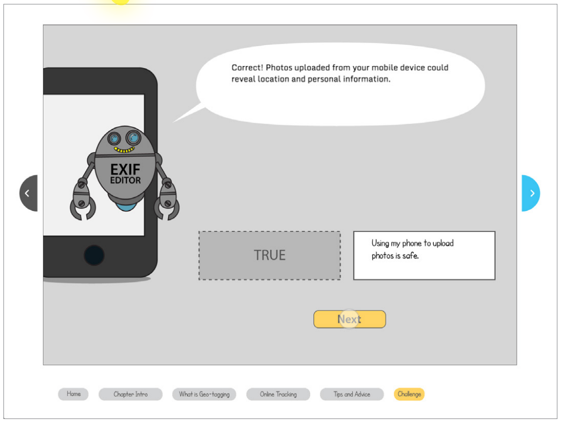
Using my phone to upload photos is safe.

Q. 2



Uh-oh. Photos uploaded from your phone could reveal more than you think! You could be sharing sensitive location based data without even realizing it!

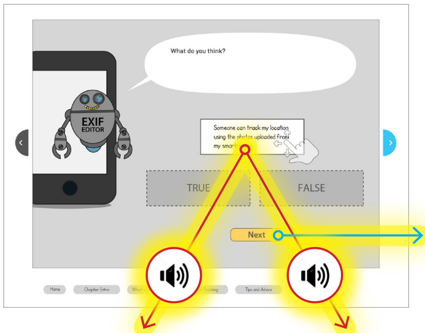
Using my phone to upload photos is safe.



Correct! Photos uploaded from your mobile device could reveal location and personal information.

Using my phone to upload photos is safe.

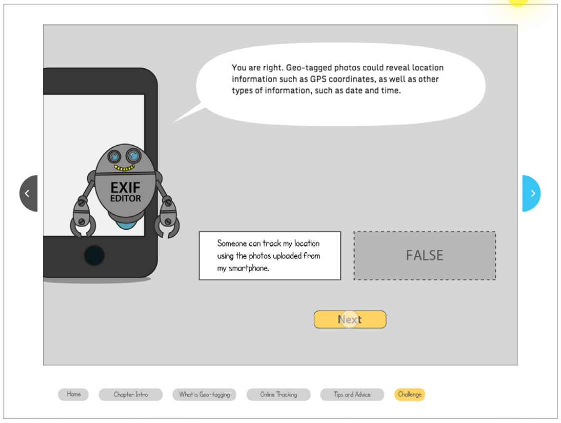
Q. 2



What do you think?

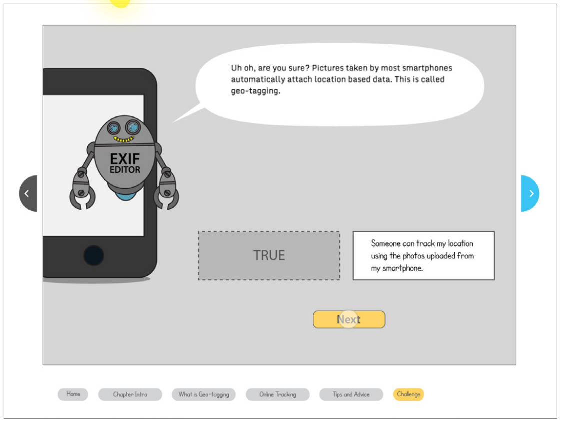
Someone can track my location using the photos uploaded from my smartphone.

Q. 3



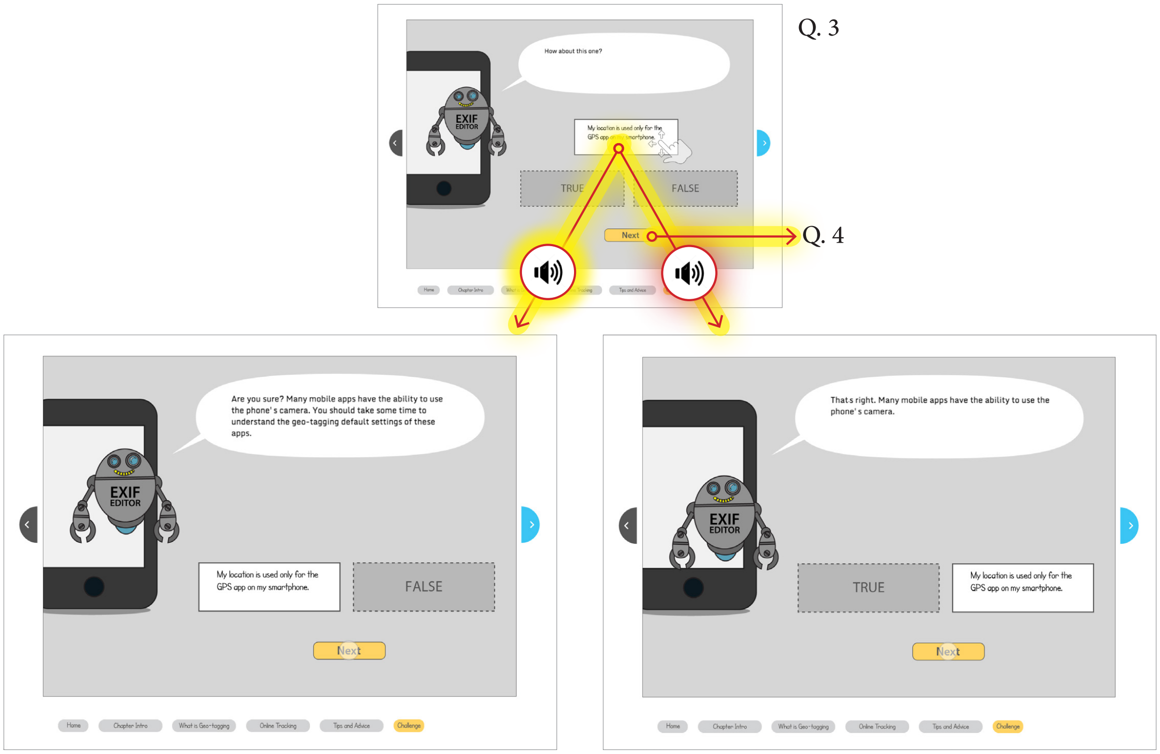
You are right. Geo-tagged photos could reveal location information such as GPS coordinates, as well as other types of information, such as date and time.

Someone can track my location using the photos uploaded from my smartphone.



Uh oh, are you sure? Pictures taken by most smartphones automatically attach location based data. This is called geo-tagging.

Someone can track my location using the photos uploaded from my smartphone.



Q. 3

Q. 4

How about this one?

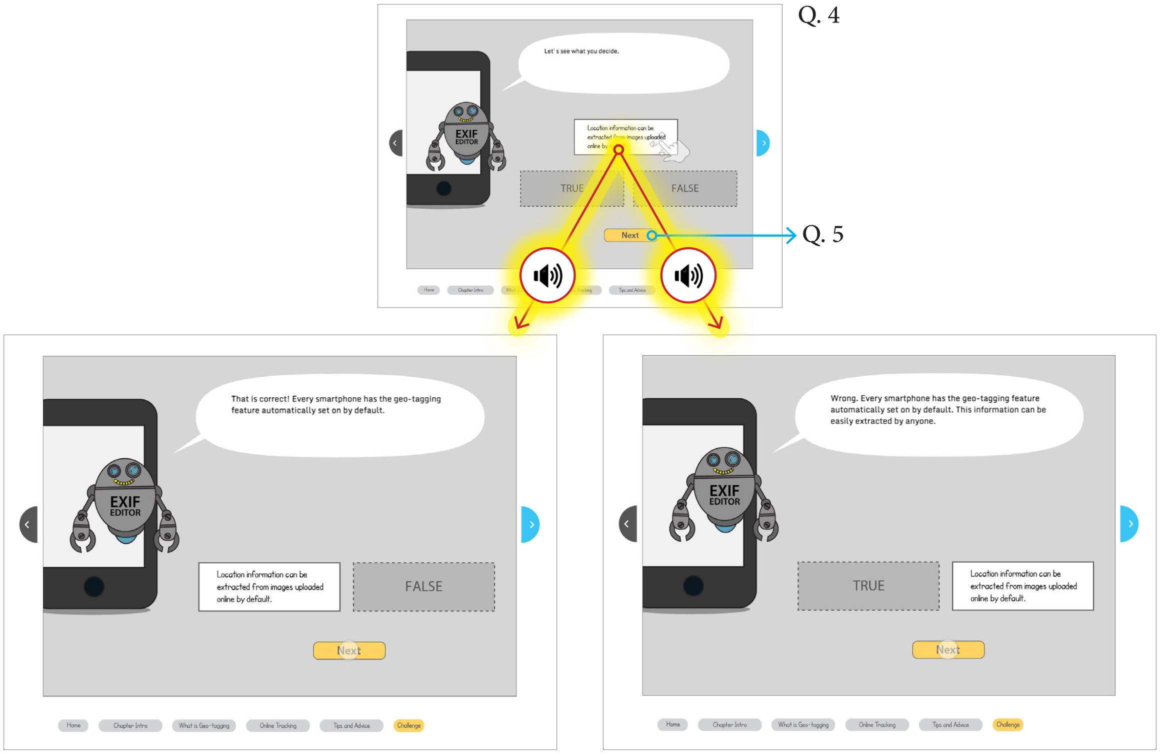
My location is used only for the GPS app on my smartphone.

Are you sure? Many mobile apps have the ability to use the phone' s camera. You should take some time to understand the geo-tagging default settings of these apps.

My location is used only for the GPS app on my smartphone.

Thats right. Many mobile apps have the ability to use the phone' s camera.

My location is used only for the GPS app on my smartphone.



Q. 4

Q. 5

Let' s see what you decide.

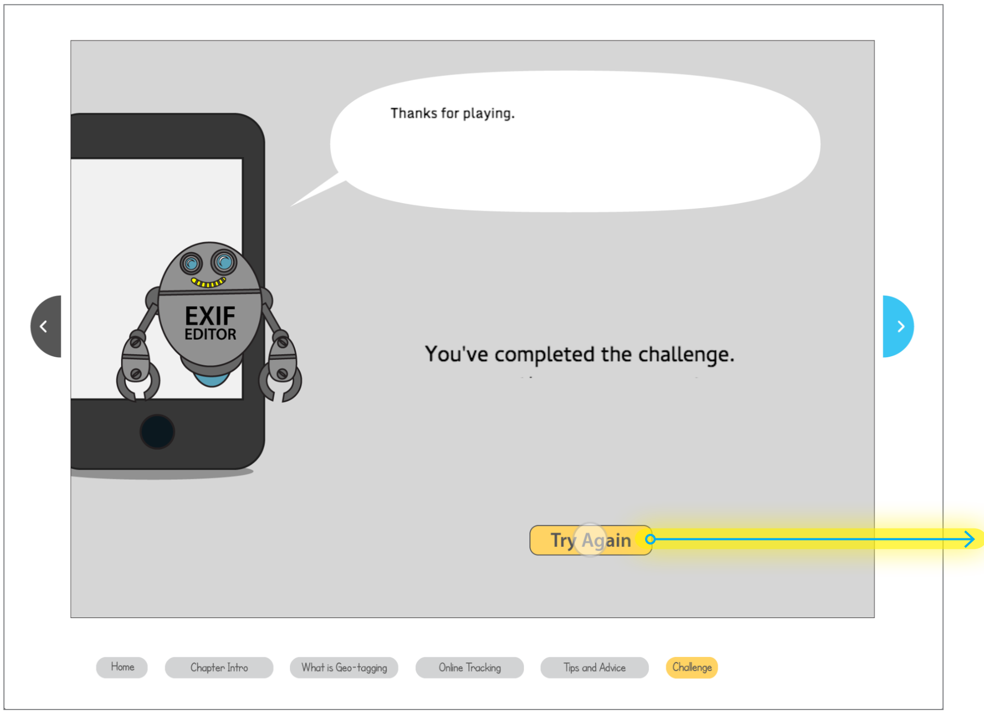
Location information can be extracted from images uploaded online by default.

That is correct! Every smartphone has the geo-tagging feature automatically set on by default.

Location information can be extracted from images uploaded online by default.

Wrong. Every smartphone has the geo-tagging feature automatically set on by default. This information can be easily extracted by anyone.

Location information can be extracted from images uploaded online by default.



Thanks for playing.

You've completed the challenge.

Q. 1

Appendix B

Cyberheroes Design Documentation

Cyberheroes Design Documentation

🔊 Sound Effect

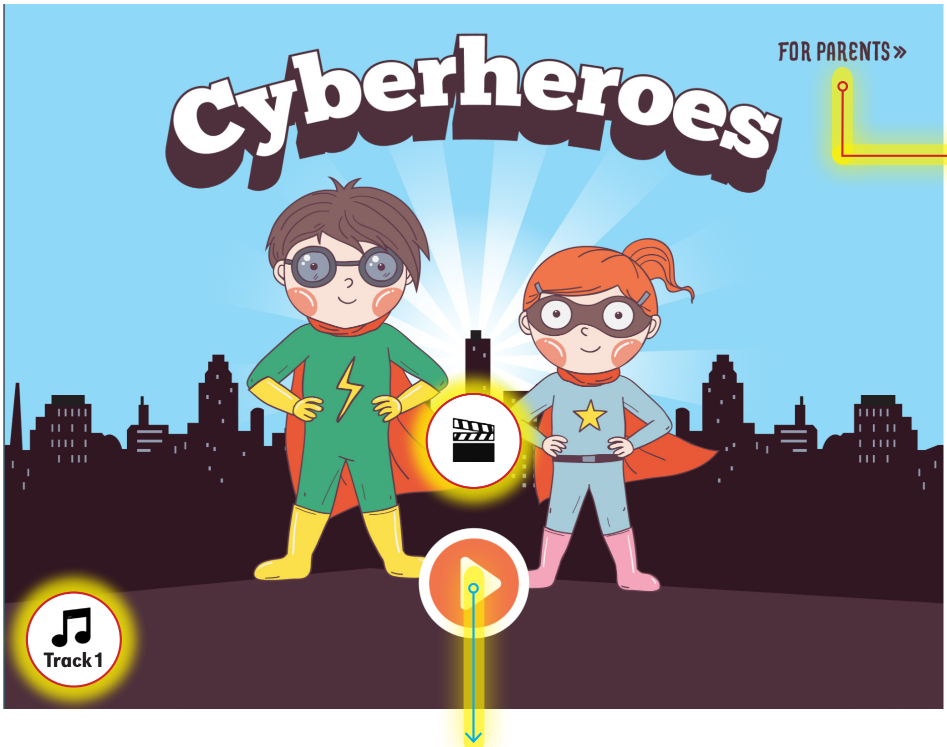
💬 Voice Effect

🎬 Animation

🎵 Backgound Music

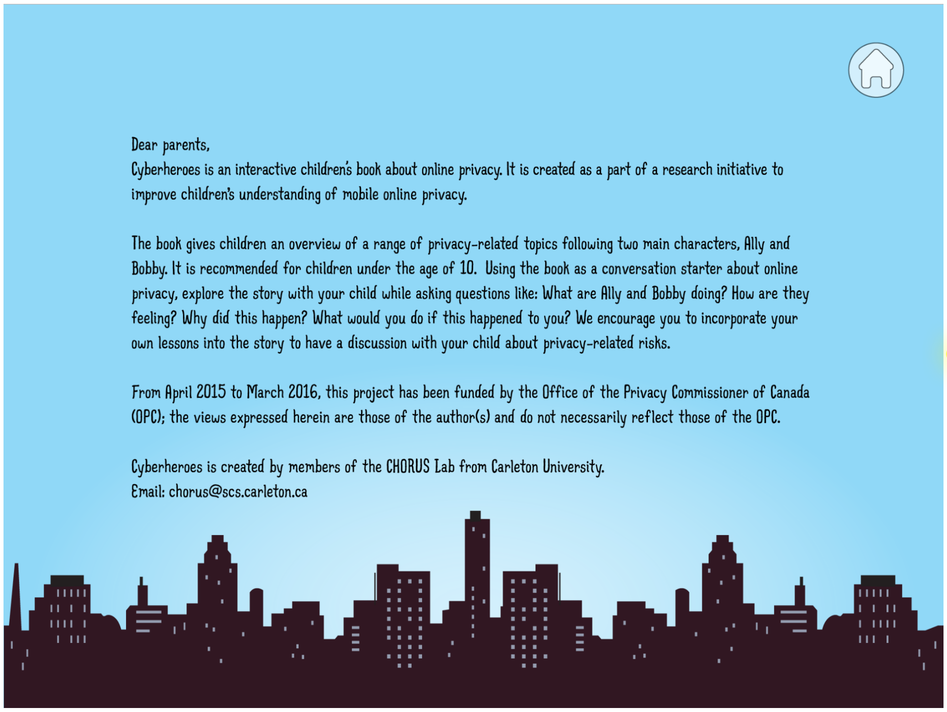
→ Navigation

→ Interaction



Landing Screen

Pg. 1

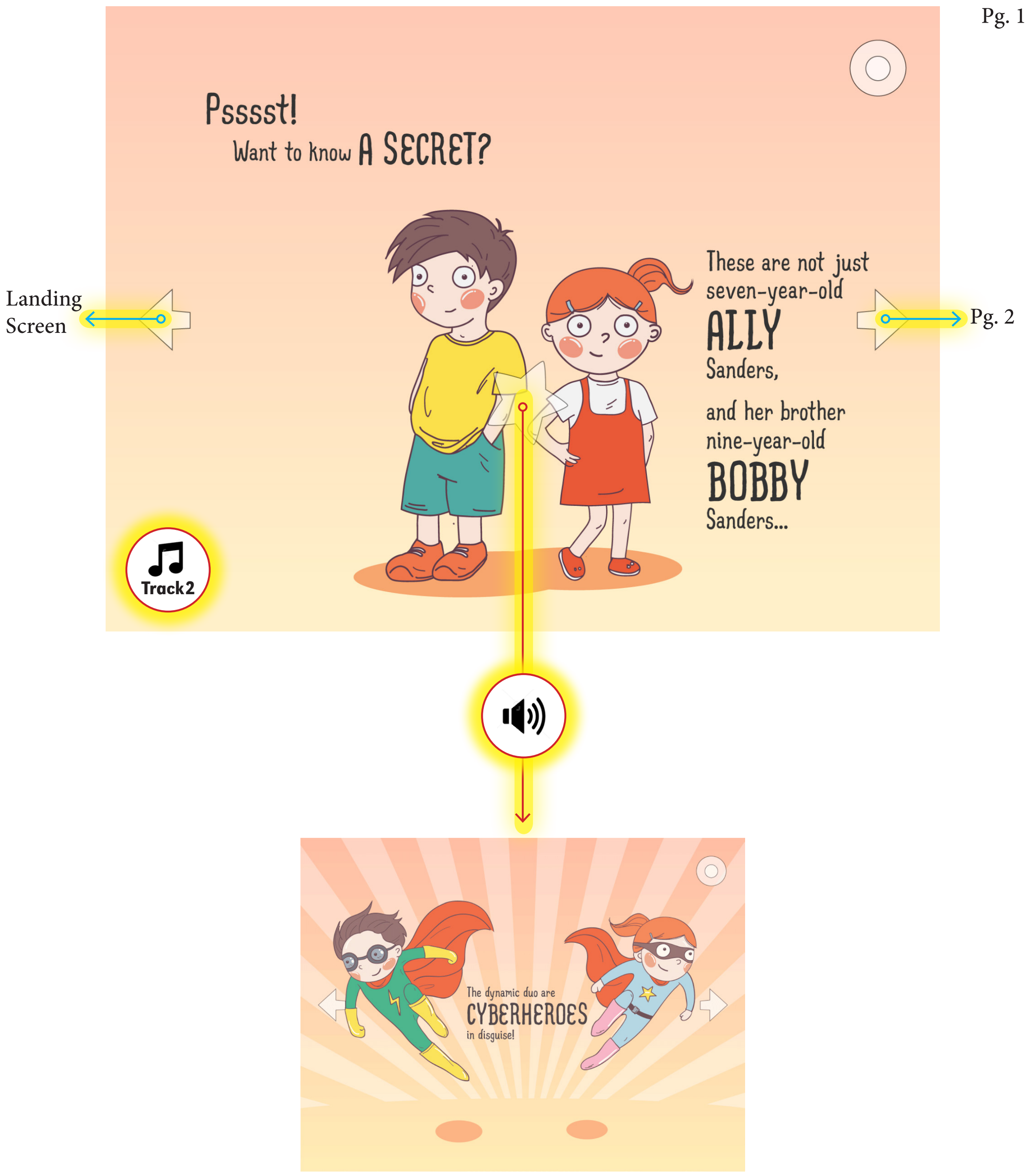


Dear parents,
Cyberheroes is an interactive children's book about online privacy. It is created as a part of a research initiative to improve children's understanding of mobile online privacy.

The book gives children an overview of a range of privacy-related topics following two main characters, Ally and Bobby. It is recommended for children under the age of 10. Using the book as a conversation starter about online privacy, explore the story with your child while asking questions like: What are Ally and Bobby doing? How are they feeling? Why did this happen? What would you do if this happened to you? We encourage you to incorporate your own lessons into the story to have a discussion with your child about privacy-related risks.

From April 2015 to March 2016, this project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

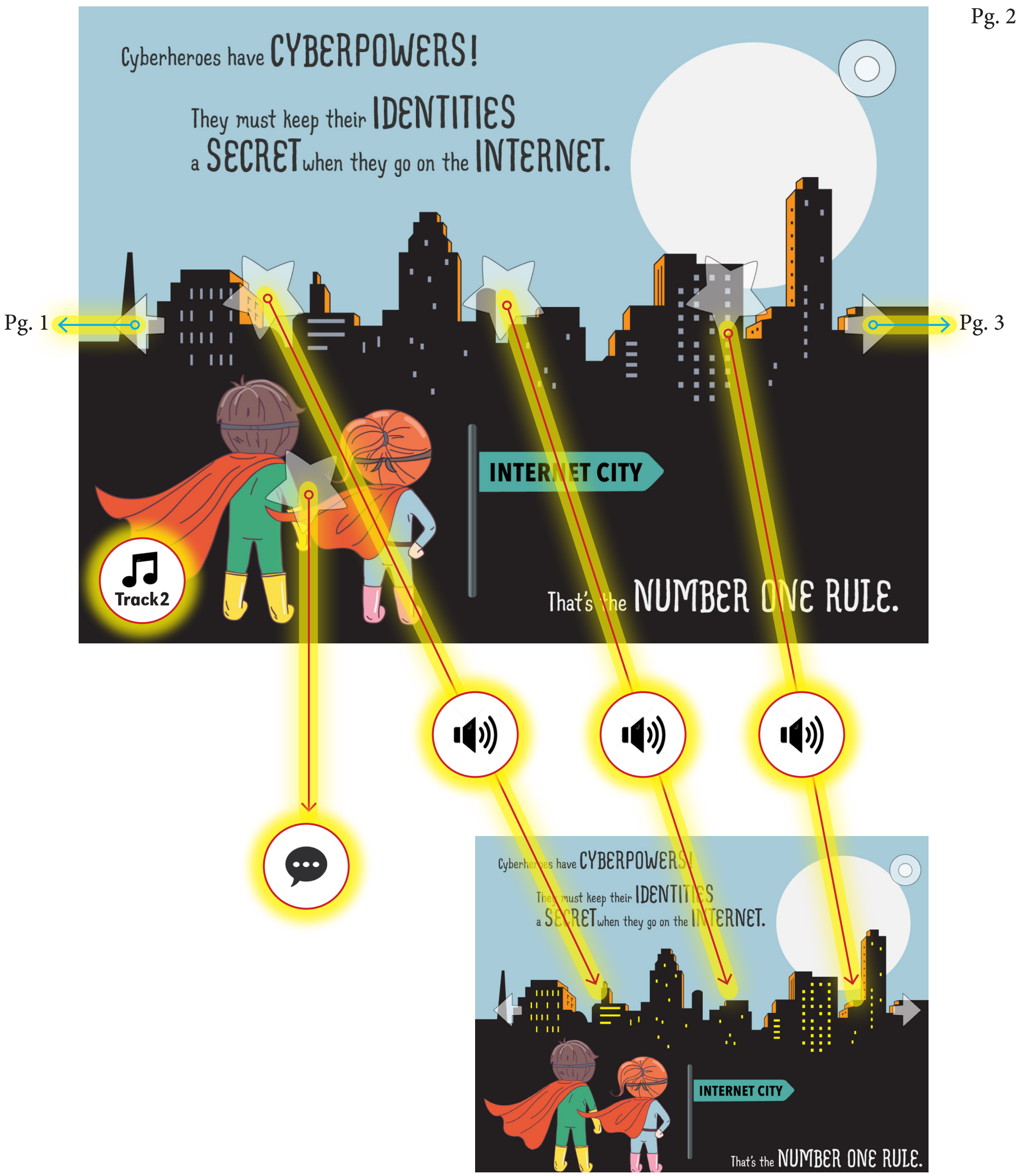
Cyberheroes is created by members of the CHORUS Lab from Carleton University.
Email: chorus@scs.carleton.ca

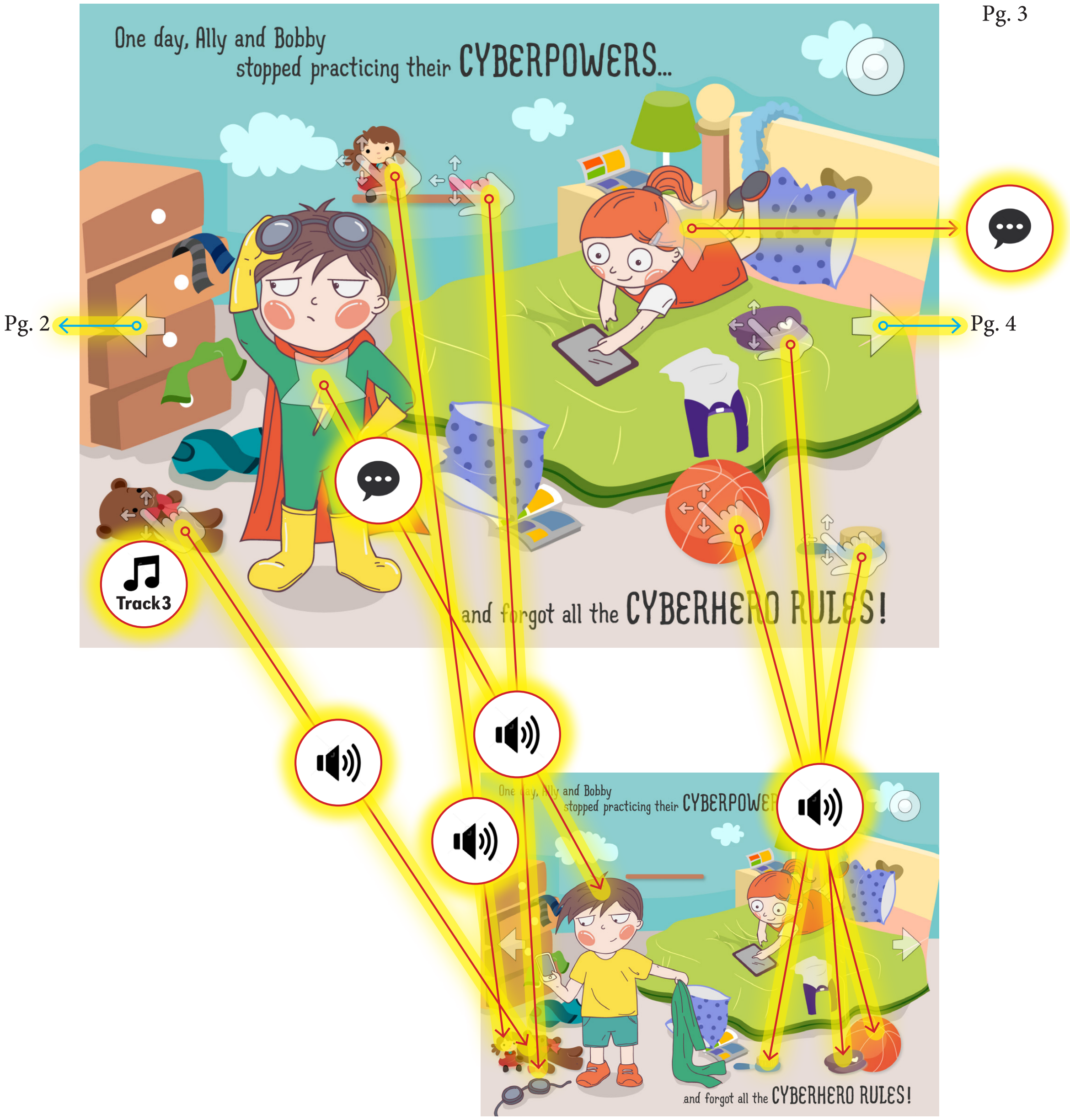


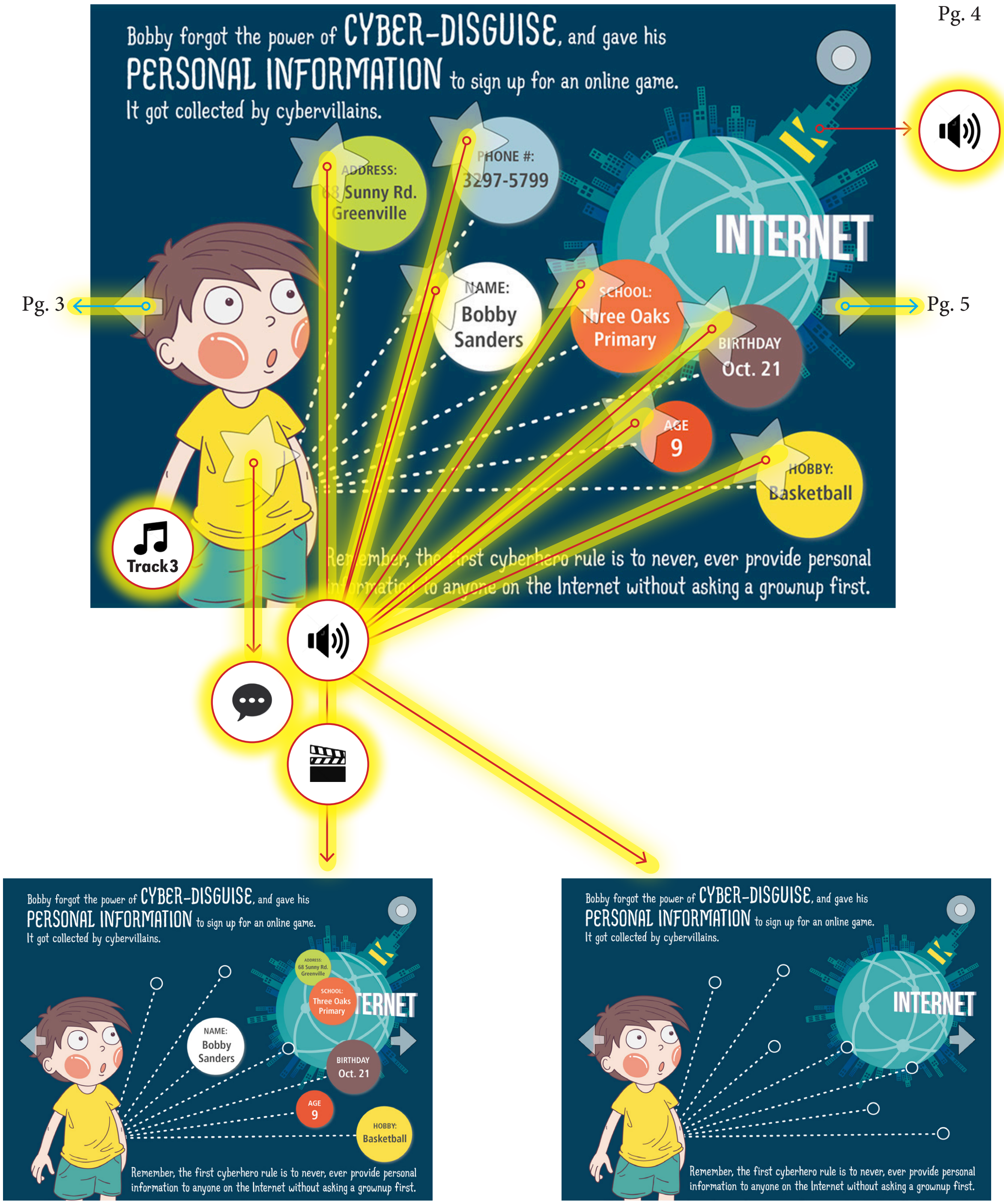
Psssst!
Want to know A SECRET?

These are not just seven-year-old ALLY Sanders, and her brother nine-year-old BOBBY Sanders...

The dynamic duo are CYBERHEROES in disguise!

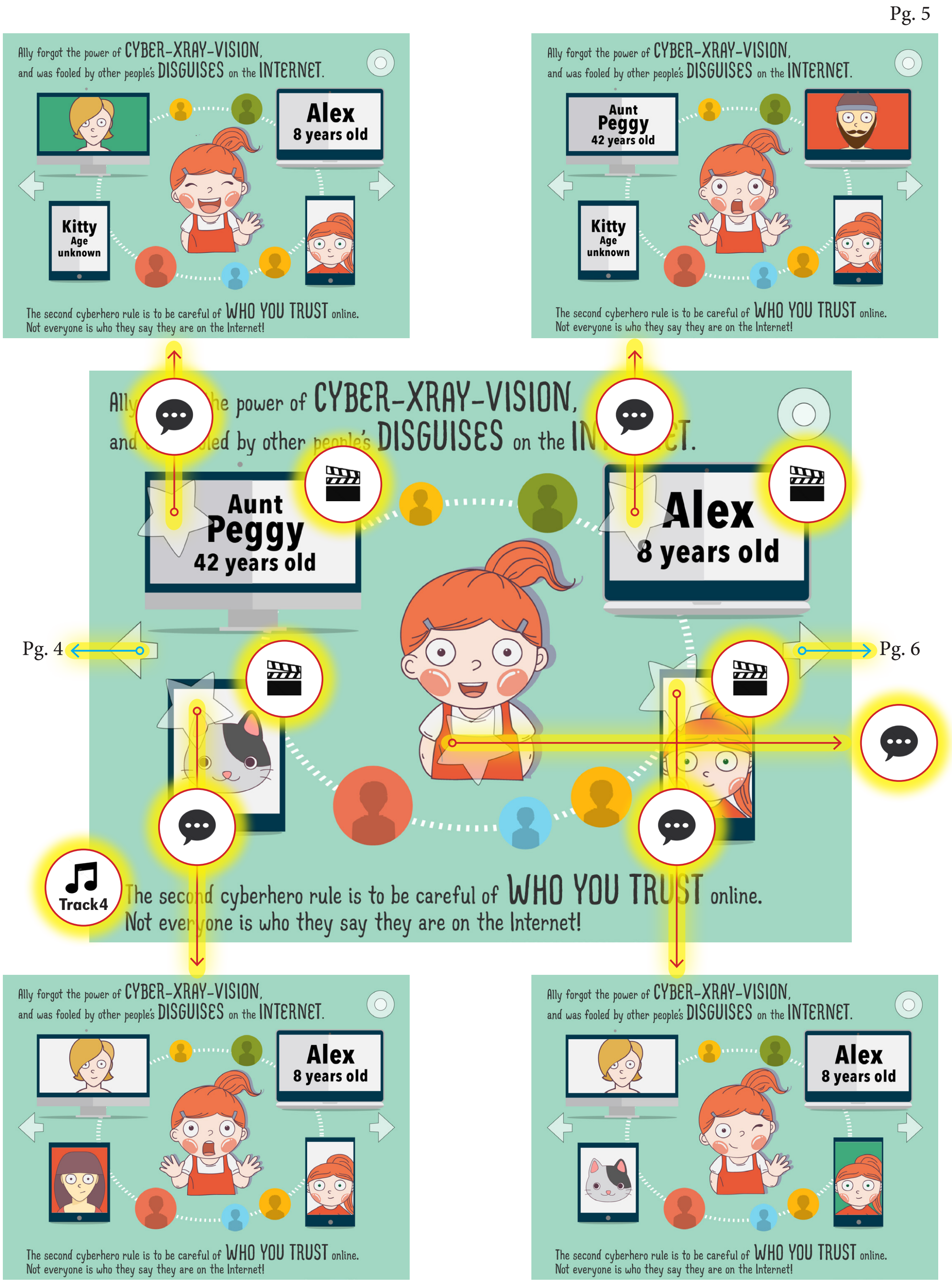

Pg. 2
Cyberheroes have CYBERPOWERS!
They must keep their IDENTITIES
a SECRET when they go on the INTERNET.
Pg. 1
Pg. 3
INTERNET CITY
Track2
That's the NUMBER ONE RULE.


Pg. 3
One day, Ally and Bobby
stopped practicing their CYBERPOWERS...
Pg. 2
Pg. 4
Track3
and forgot all the CYBERHERO RULES!
One day, Ally and Bobby
stopped practicing their CYBERPOWE
and forgot all the CYBERHERO RULES!



Bobby forgot the power of CYBER-DISGUISE, and gave his PERSONAL INFORMATION to sign up for an online game. It got collected by cybervillains.

Remember, the first cyberhero rule is to never, ever provide personal information to anyone on the Internet without asking a grownup first.



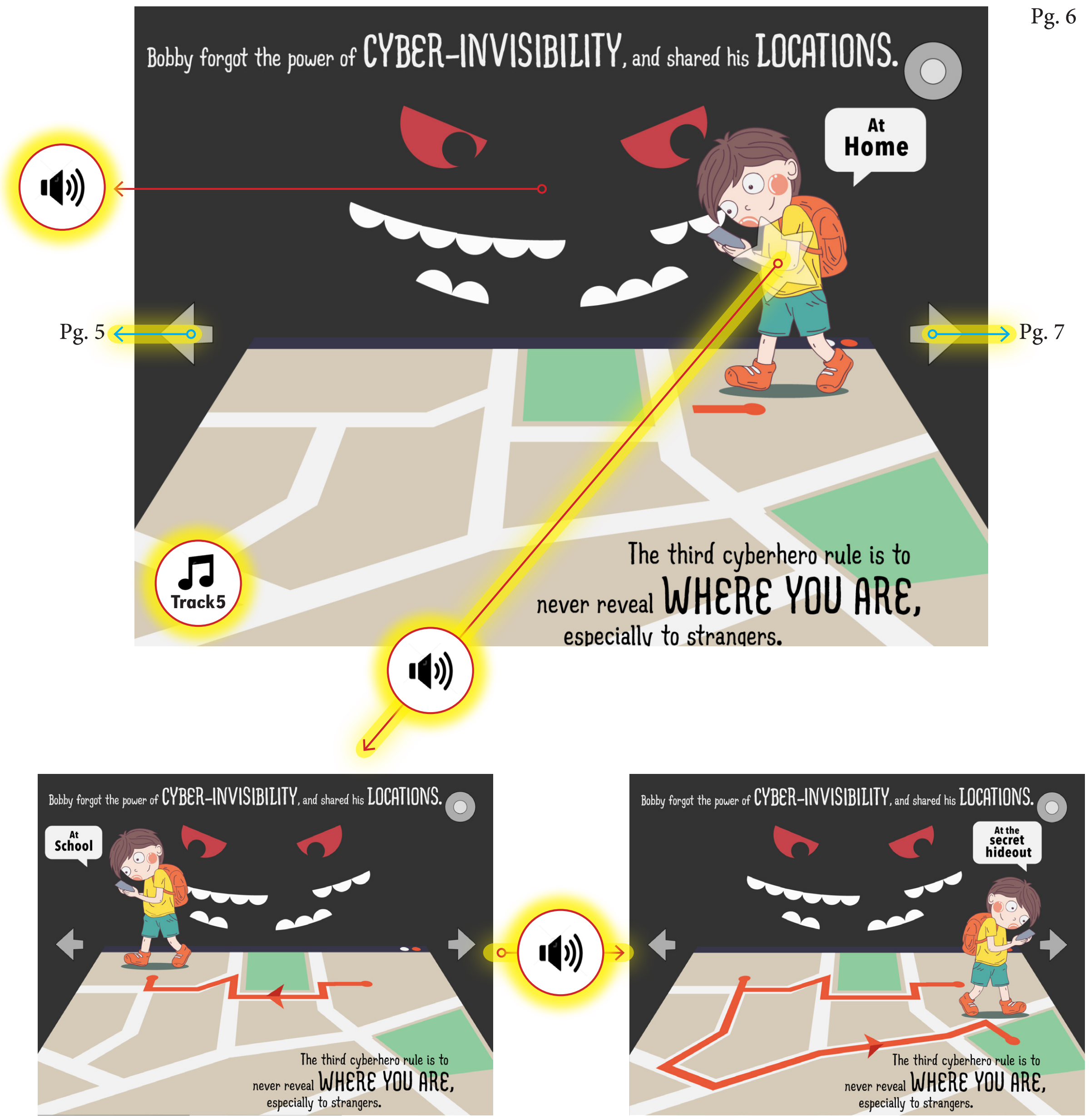
Ally forgot the power of CYBER-XRAY-VISION, and was fooled by other people's DISGUISES on the INTERNET.

The second cyberhero rule is to be careful of WHO YOU TRUST online. Not everyone is who they say they are on the Internet!

Ally forgot the power of CYBER-XRAY-VISION, and was fooled by other people's DISGUISES on the INTERNET.

The second cyberhero rule is to be careful of WHO YOU TRUST online. Not everyone is who they say they are on the Internet!

Pg. 6



Bobby forgot the power of CYBER-INVISIBILITY, and shared his LOCATIONS.

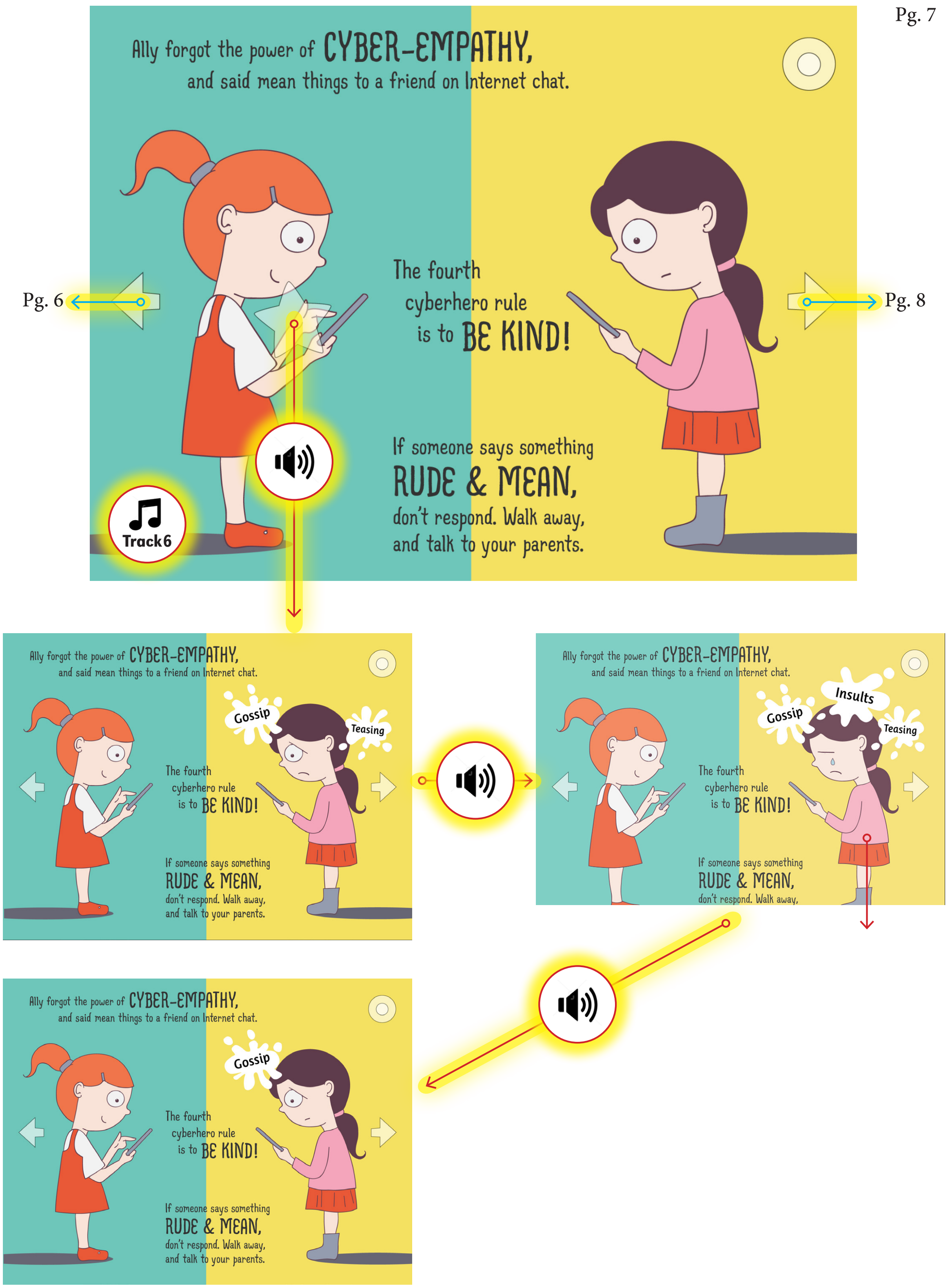
The third cyberhero rule is to never reveal WHERE YOU ARE, especially to strangers.

Bobby forgot the power of CYBER-INVISIBILITY, and shared his LOCATIONS.

The third cyberhero rule is to never reveal WHERE YOU ARE, especially to strangers.

Bobby forgot the power of CYBER-INVISIBILITY, and shared his LOCATIONS.

The third cyberhero rule is to never reveal WHERE YOU ARE, especially to strangers.

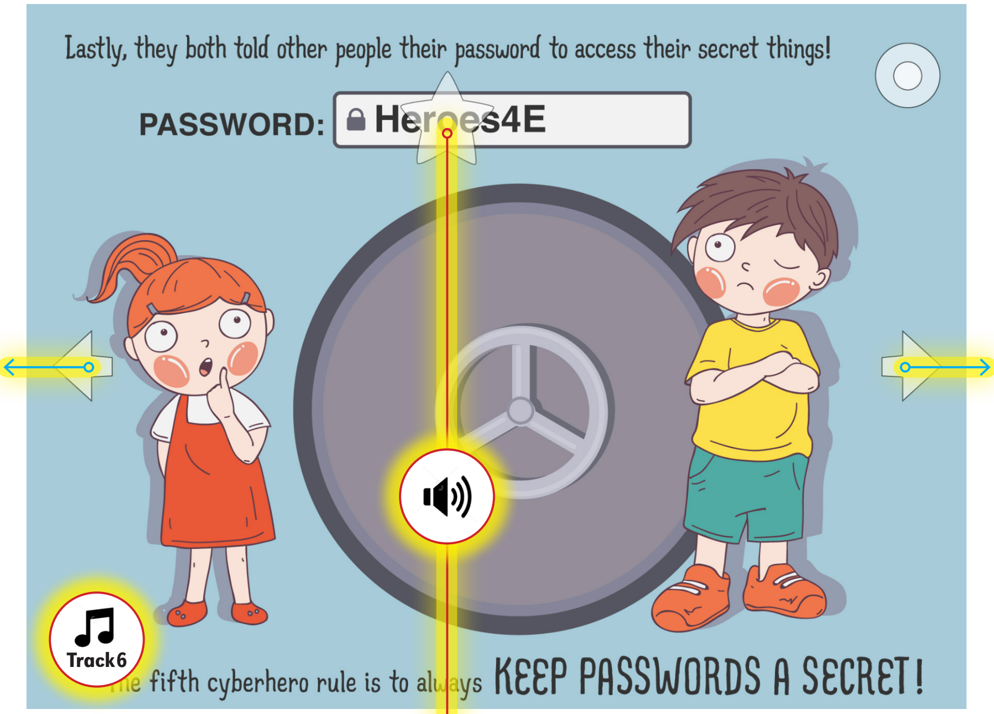


Ally forgot the power of CYBER-EMPATHY,
and said mean things to a friend on Internet chat.

The fourth
cyberhero rule
is to BE KIND!

If someone says something
RUDE & MEAN,
don't respond. Walk away,
and talk to your parents.

Pg. 8



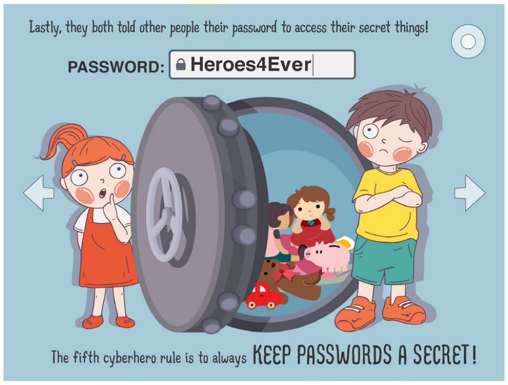
Lastly, they both told other people their password to access their secret things!

PASSWORD: Heroes4E

The fifth cyberhero rule is to always KEEP PASSWORDS A SECRET!

Pg. 7

Pg. 8

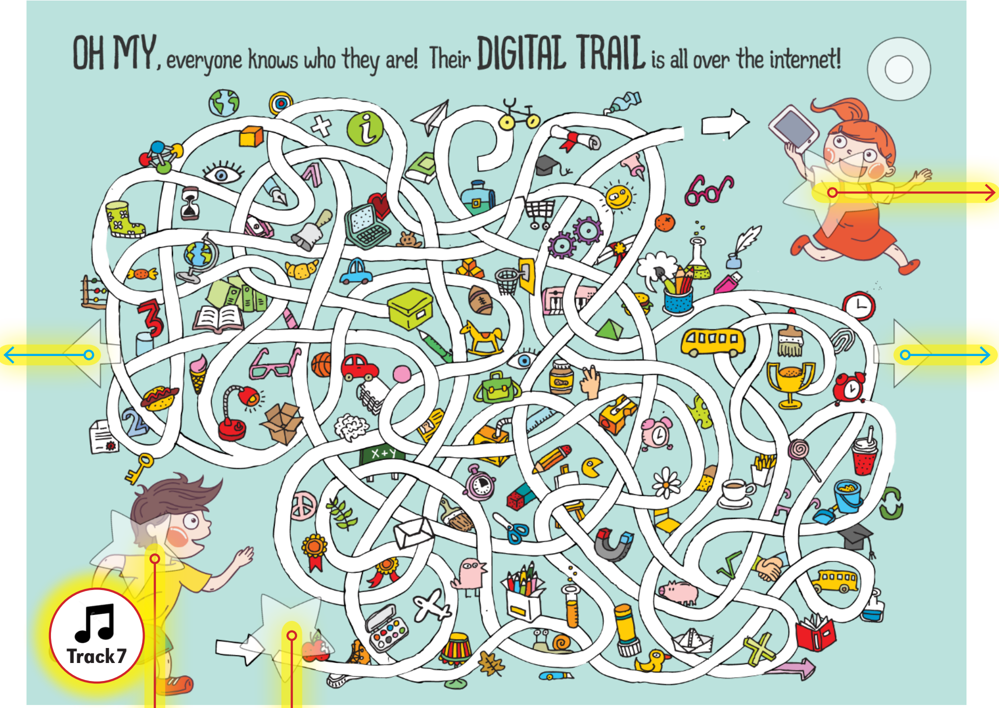


Lastly, they both told other people their password to access their secret things!

PASSWORD: Heroes4Ever

The fifth cyberhero rule is to always KEEP PASSWORDS A SECRET!

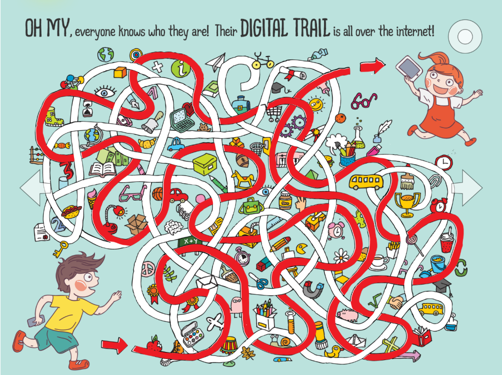
Pg. 9


OH MY, everyone knows who they are! Their DIGITAL TRAIL is all over the internet!

Pg. 8

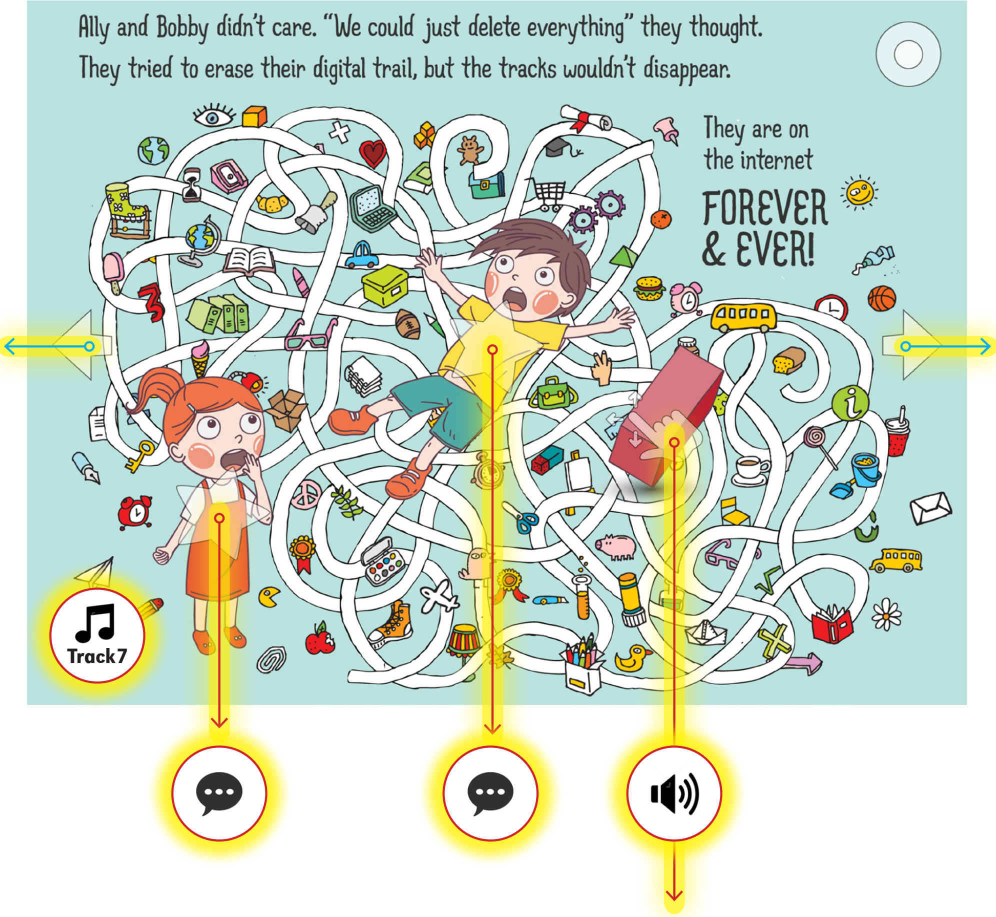
Pg. 10

Track7


OH MY, everyone knows who they are! Their DIGITAL TRAIL is all over the internet!

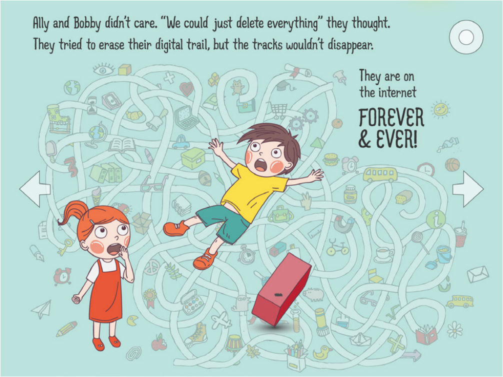
Pg. 10

Pg. 9



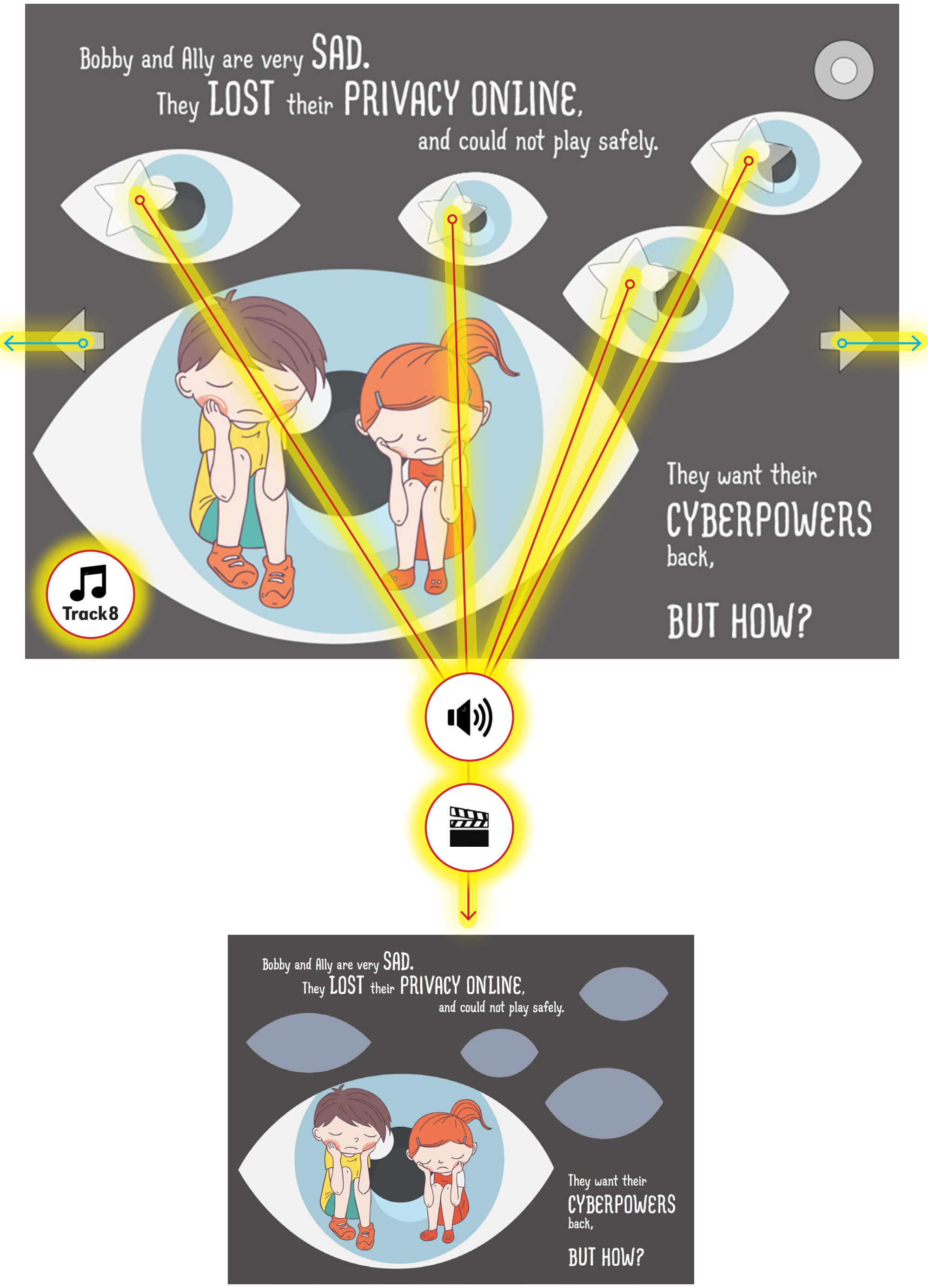
Ally and Bobby didn't care. "We could just delete everything" they thought. They tried to erase their digital trail, but the tracks wouldn't disappear.

Pg. 11



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

Pg. 11



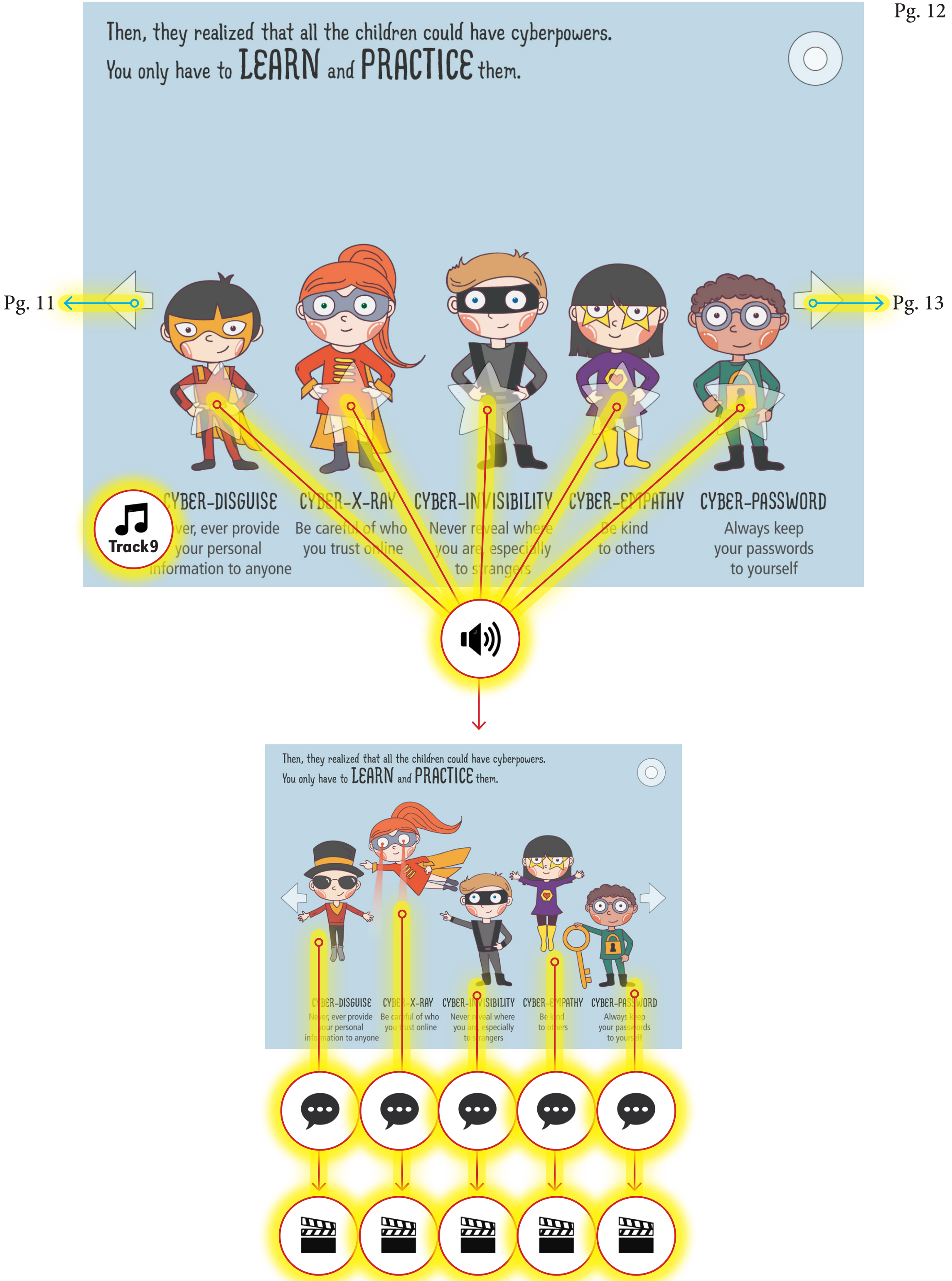
Pg. 10

Pg. 12

Bobby and Ally are very SAD.
They LOST their PRIVACY ONLINE,
and could not play safely.

They want their
CYBERPOWERS
back,

BUT HOW?



Then, they realized that all the children could have cyberpowers.
You only have to LEARN and PRACTICE them.

CYBER-DISGUISE
Never, ever provide your personal information to anyone

CYBER-X-RAY
Be careful of who you trust online

CYBER-INVISIBILITY
Never reveal where you are, especially to strangers

CYBER-EMPATHY
Be kind to others

CYBER-PASSWORD
Always keep your passwords to yourself

Then, they realized that all the children could have cyberpowers.
You only have to LEARN and PRACTICE them.

CYBER-DISGUISE
Never, ever provide your personal information to anyone

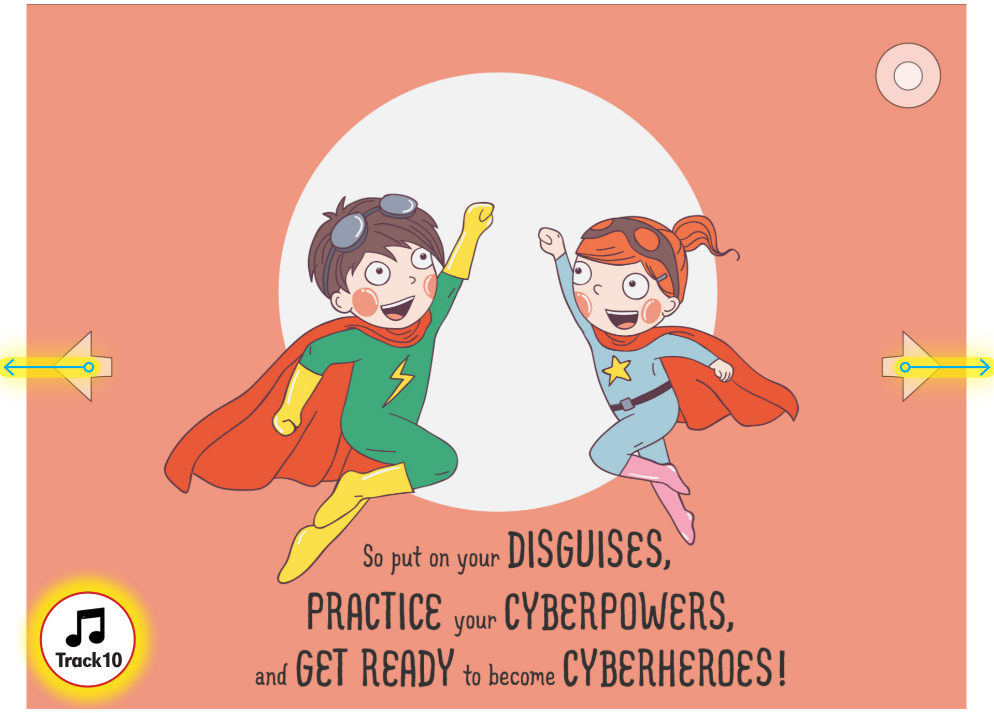
CYBER-X-RAY
Be careful of who you trust online

CYBER-INVISIBILITY
Never reveal where you are, especially to strangers

CYBER-EMPATHY
Be kind to others

CYBER-PASSWORD
Always keep your passwords to yourself

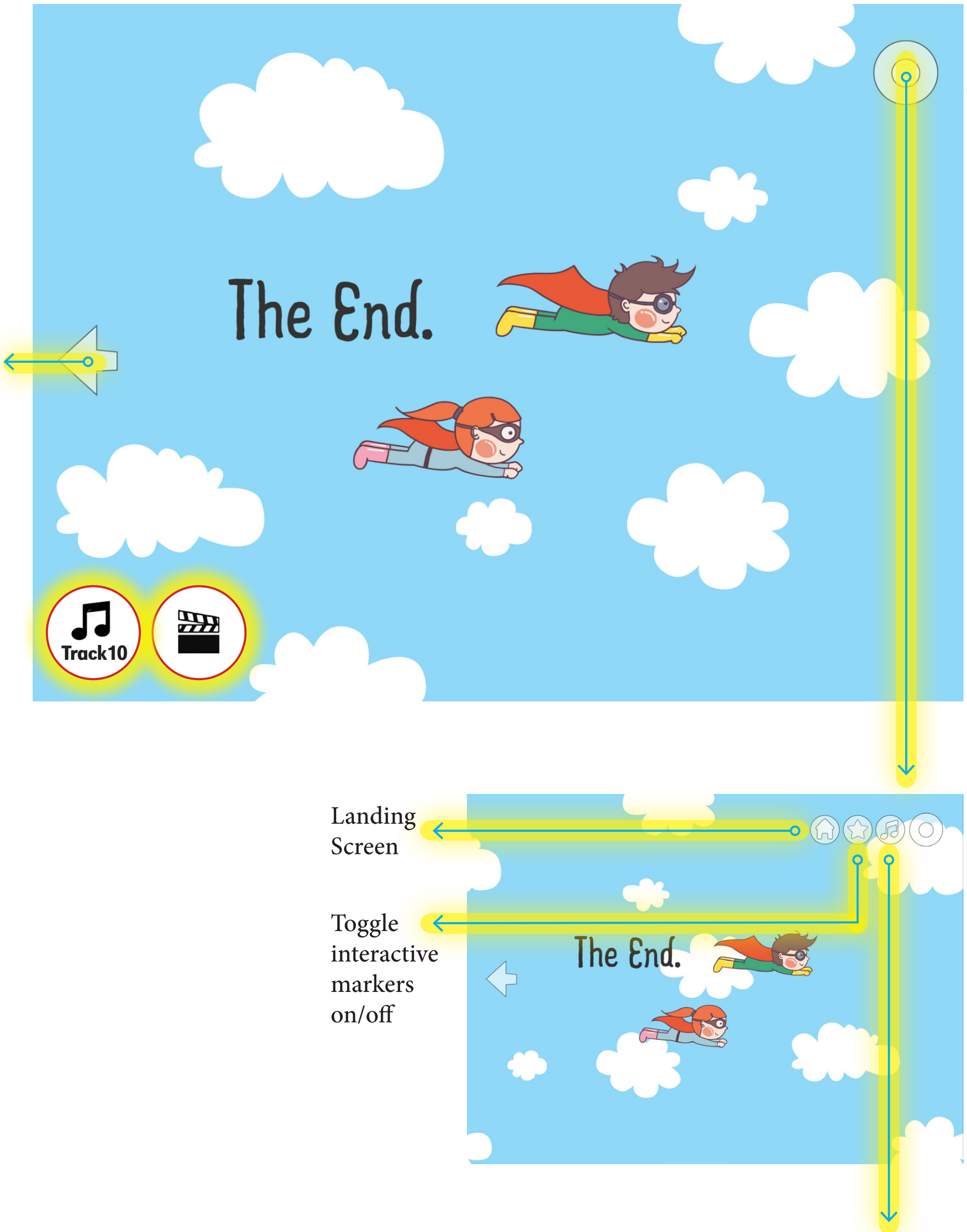
Pg. 13



So put on your DISGUISES, PRACTICE your CYBERPOWERS, and GET READY to become CYBERHEROES!

Pg. 12

Pg. 14



Pg. 14

Menu

Pg. 13

Landing Screen

Toggle interactive markers on/off

Toggle sound on/off

Appendix C

Secure Comics User Study Material

C.1: Pre- and Post-Test Interview with Children

{The following questions will be used twice, first as a pre-test, and second as a post-test.}

Question Group A:

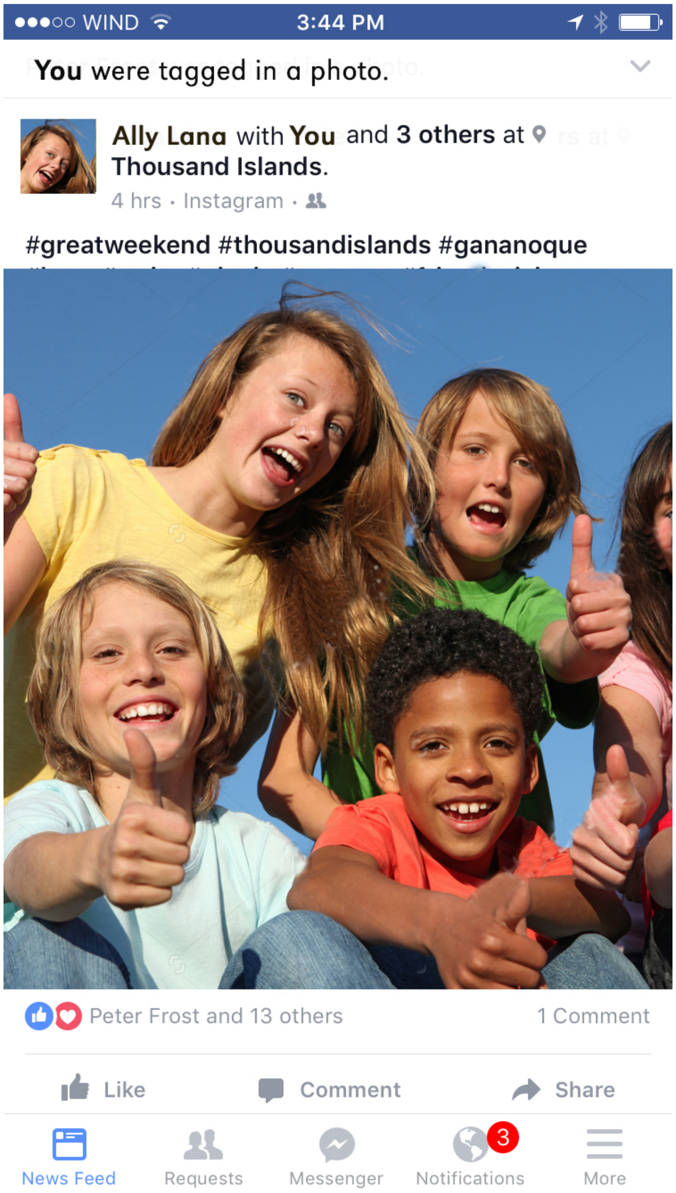
1. What is online privacy?
2. What is online tracking?
    a. Can you give some examples of the ways people could be tracked online on a smartphone?
3. What is Geo-tagging on your smartphone?
    a. Can you give me some examples of the types of file or data that could be geo-tagged?
4. What could you do to protect yourself from geo-tagging and online tracking?

Question Group B:

1. How does your smartphone track your location?
2. How could someone track your location using photos uploaded from your smartphone?
3. How could someone track other people's location using photos uploaded from your smartphone?
4. What are some of the possible negative outcomes of being tracked on a smartphone?

Question Group C (starts on the following page)

Question Group C:
Images were used as visual aids for the participants when the questions were asked.



You were tagged in a photo.

Ally Lana with You and 3 others at Thousand Islands.

4 hrs · Instagram ·

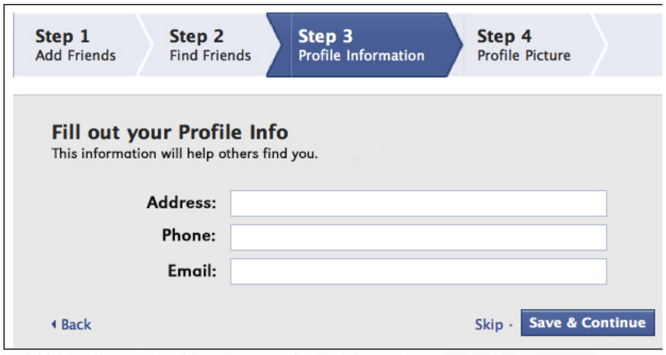
#greatweekend #thousandislands #gananoque

Peter Frost and 13 others

1 Comment

1. You took a group picture with your friends on a trip together and one of them asked you to post the picture online, check-in your location, and tag everyone in it.

   a) What would you do in this situation?
   b) How might this affect your privacy?
   c) How might this affect other's privacy?

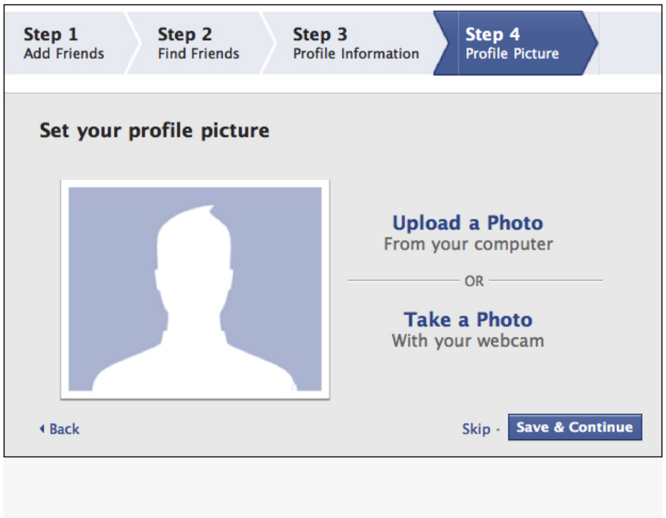


Fill out your Profile Info
This information will help others find you.

Address:

Phone:

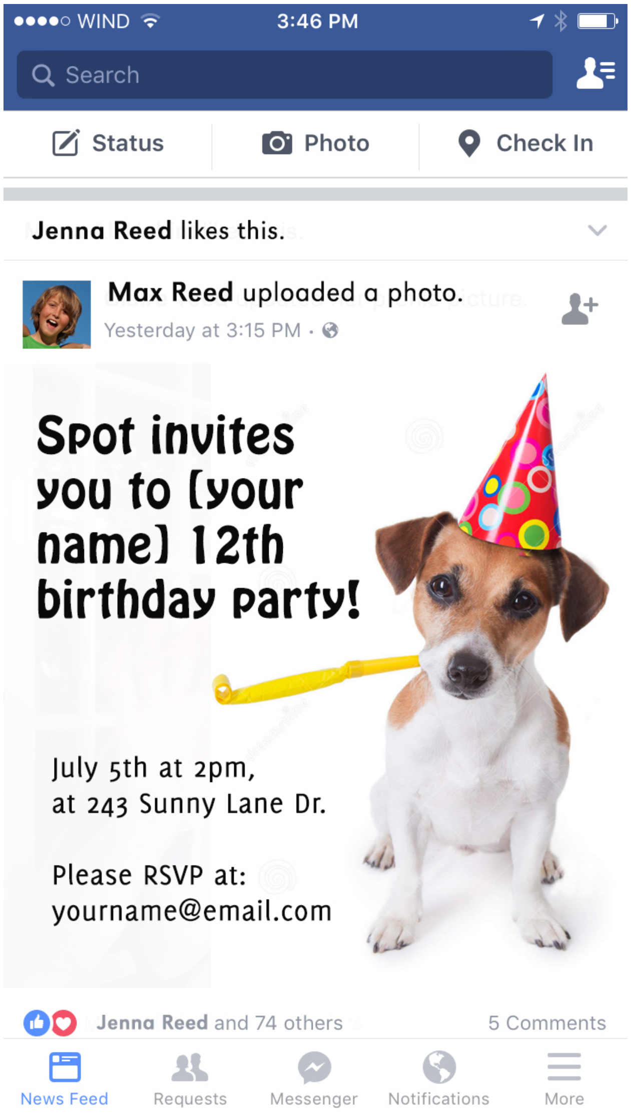
Email:



Set your profile picture

2. Suppose you want to sign up for a new social media account. It requests you to upload a picture of yourself with your address, phone number, and email address so other members of the website can contact you.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other's privacy?



Jenna Reed likes this.

Max Reed uploaded a photo.
Yesterday at 3:15 PM ·

Spot invites you to (your name) 12th birthday party!

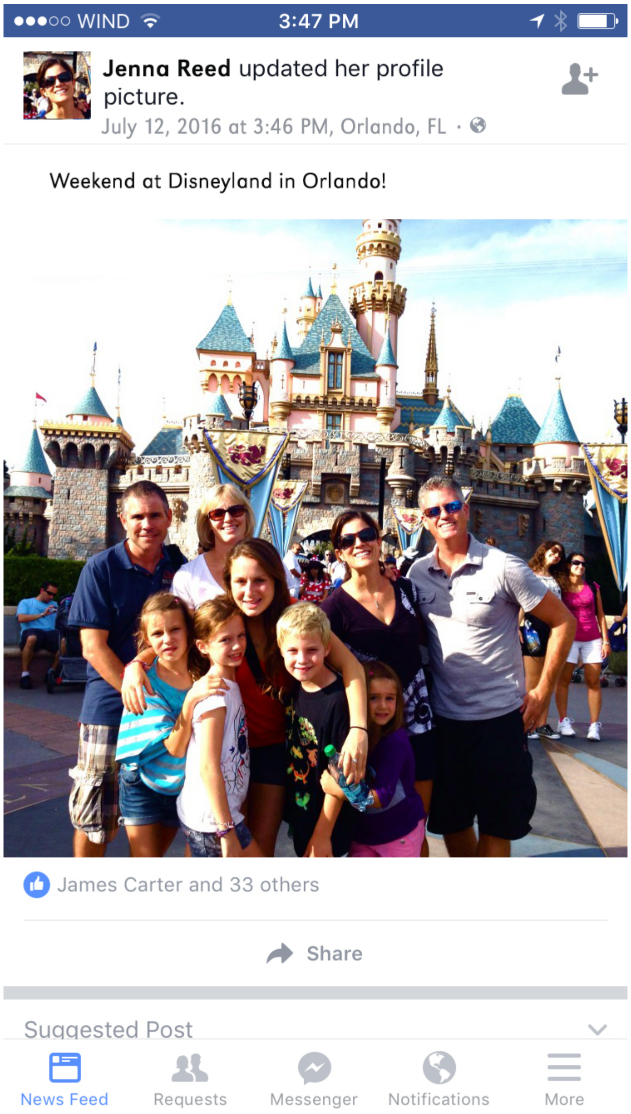
July 5th at 2pm,
at 243 Sunny Lane Dr.

Please RSVP at:
yourname@email.com

Jenna Reed and 74 others 5 Comments

3) Your best friend created an invitation on social media to your upcoming birthday party that contained a picture of his/her dog wearing a birthday hat, and the following message: “Spot invites you to [your name]12th birthday party on July 5th at 2pm, at 243 Sunny Lane Dr., please RSVP at yourname@email.com.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other’s privacy?



Jenna Reed updated her profile picture.
July 12, 2016 at 3:46 PM, Orlando, FL ·

Weekend at Disneyland in Orlando!

James Carter and 33 others

4) You are at Disneyland with your family and your friend's family. You saw a picture that your friend's mom posted on social media that contained the following: An image of their family with you and your family, and a comment that says, "Weekend with friends at Disneyland in Orlando!" and the date.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other's privacy?

C.2: One-Week Interview with Children

(Question groups A and B were reused from the pre/post tests. Question group C contained alternate scenarios from the pre/post tests.)

Question Group A:

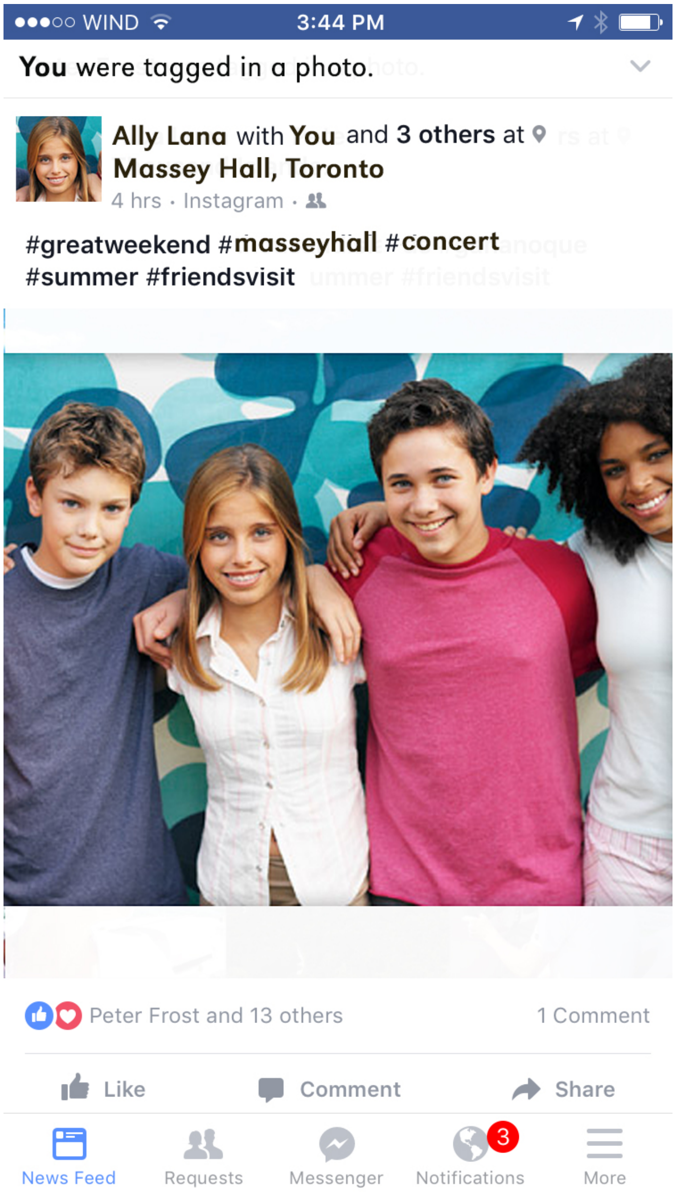
5. What is online privacy?
6. What is online tracking?
    a. Can you give some examples of the ways people could be tracked online on a smartphone?
7. What is Geo-tagging on your smartphone?
    a. Can you give me some examples of the types of file or data that could be geo-tagged?
8. What could you do to protect yourself from geo-tagging and online tracking?

Question Group B:

5. How does your smartphone track your location?
6. How could someone track <u>your</u> location using photos uploaded from your smartphone?
7. How could someone track other people's location using photos uploaded from your smartphone?
8. What are some of the possible negative outcomes of being tracked on a smartphone?

Question Group C (starts on the following page)

Question Group C:



You were tagged in a photo.

Ally Lana with You and 3 others at Massey Hall, Toronto

4 hrs · Instagram ·

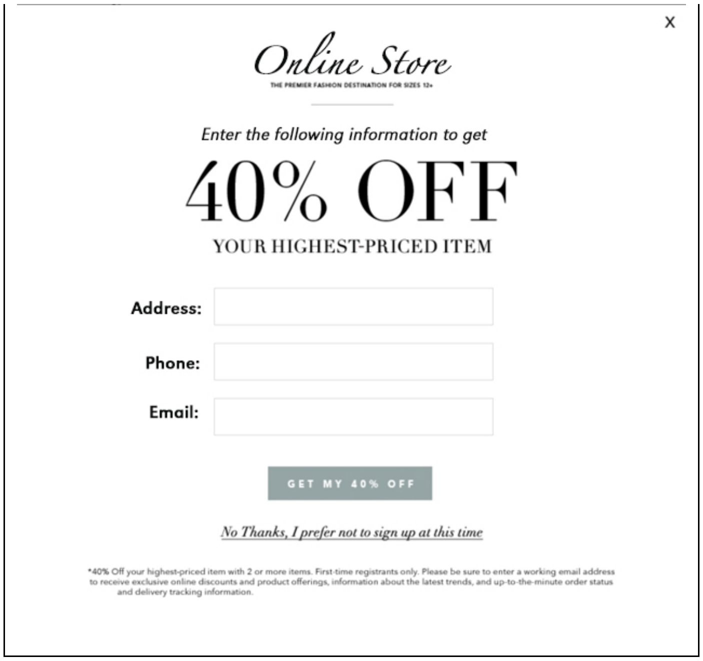
#greatweekend #masseyhall #concert #summer #friendsvisit

Peter Frost and 13 others

1 Comment

1) You took a group picture at a concert with your friends. One of them asked you to post the picture online, check-in your location, and tag everyone in it.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other's privacy?



THE PREMIER FASHION DESTINATION FOR SIZES 12+

Enter the following information to get

40% OFF

YOUR HIGHEST-PRICED ITEM

Address:

Phone:

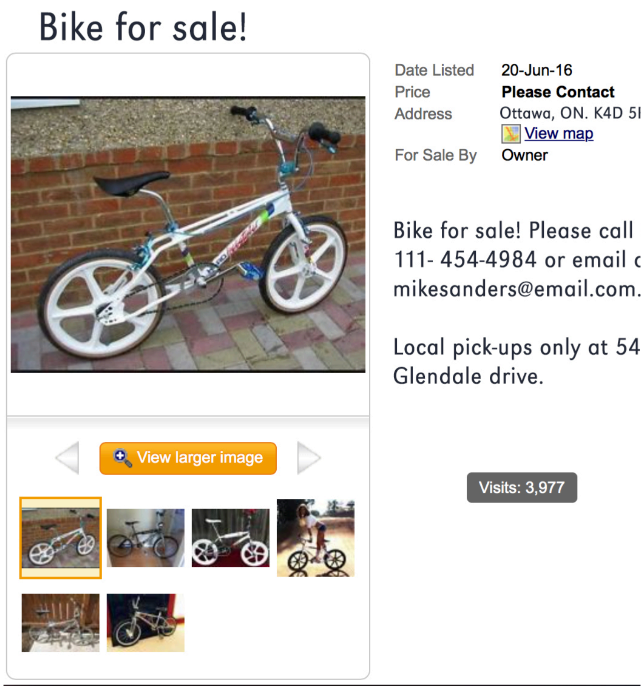
Email:

No Thanks, I prefer not to sign up at this time

*40% Off your highest-priced item with 2 or more items. First-time registrants only. Please be sure to enter a working email address to receive exclusive online discounts and product offerings, information about the latest trends, and up-to-the-minute order status and delivery tracking information.

2) You received a pop-up from your favourite online store. It offers you 40% off on your next purchase if you enter your address, phone number, and email.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other's privacy?



Bike for sale!

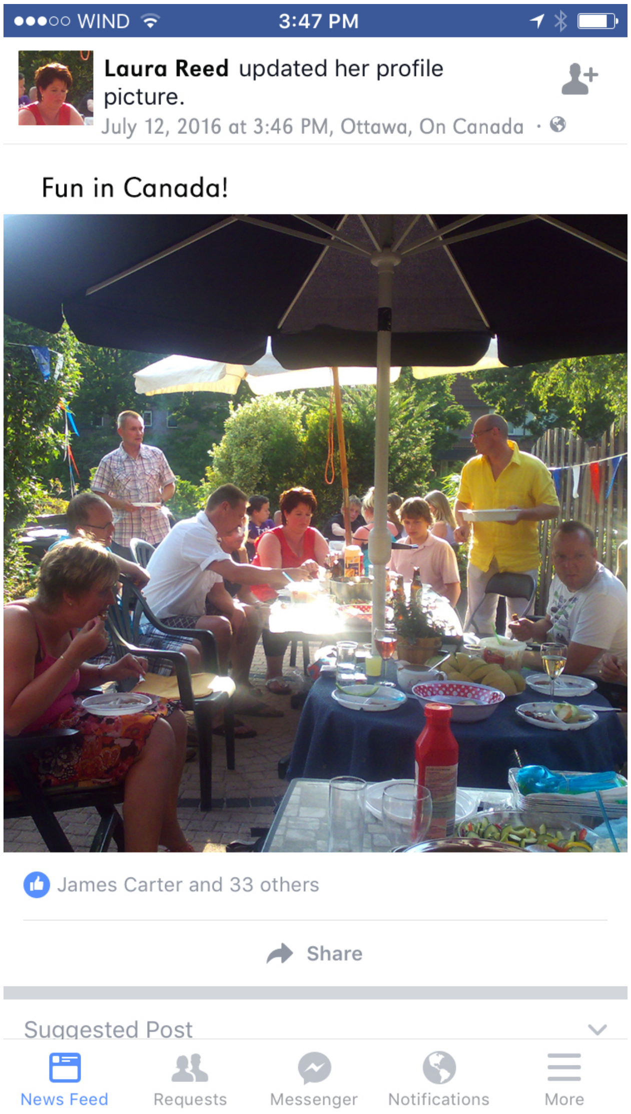
Date Listed	20-Jun-16
Price	**Please Contact**
Address	Ottawa, ON. K4D 5I View map
For Sale By	Owner

Bike for sale! Please call 111- 454-4984 or email c mikesanders@email.com.

Local pick-ups only at 54 Glendale drive.

3) Your brother/sister posted an advertisement online to sell his/her bike. The ad contained multiple images of the bike and one image of your brother/sister riding the bike. It also included your home phone number, your dad’s email, and your address. The message says. “Bike for sale! Please call at 111- 454-4984 or email at mikesanders@email.com. Local pick-ups only at 54 Glendale drive.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other’s privacy?



Laura Reed updated her profile picture.
July 12, 2016 at 3:46 PM, Ottawa, On Canada ·

Fun in Canada!

James Carter and 33 others

4) Your relatives who live in another country came to visit your family. You saw a picture they posted on social media that contained the following: An image of a bbq at your house with your family, and a comment that says, “Fun in Canada!” and the date.

a) What would you do in this situation?
b) How might this affect your privacy?
c) How might this affect other’s privacy?

C.3: Children's Post-Evaluation Questionnaire

For each question, please circle the word that best describes your answer.

1. Would you read the comic book again?

No	**Maybe**	**Yes**

2. How fun was the comic book?

Very Boring	**Boring**	**Neither**	**Fun**	**Very Fun**

3. How easy was it to use the comic book?

Very Hard	**Hard**	**Neither**	**Easy**	**Very Easy**

4. How well did you learn from the comic book?

Very Bad	**Bad**	**Neither**	**Well**	**Very well**

5. How likeable were the characters?

Very Dislikeable

Dislikeable

Neither

Likeable

Very Likable

6. How willing would you be to show the comic book to other kids?

Very Unwilling

Unwilling

Neither

Willing

Very Willing

7. What did you like about the comic book?

8. What did you dislike about the comic book?

C.4: Children's Demographic Questionnaire (Completed by Parents)

Please select or give the most accurate answer to each question below.

1. What is your child's age?

□ 11 yrs □ 12 yrs □ 13 yrs

---

2. What grade is your child in school?

□ Grade 6 □ Grade 7 □ Grade 8 □ Other: ________

---

3. What is your child's gender?

□ Male □ Female

---

4. How long does your child spend on mobile device(s) daily?

□ 20min or less □ 40min or less □ 1 hr □ 2 hrs □ 3 hrs or more

---

5. How long does your child go online daily?

□ 20min or less □ 40min or less □ 1 hr □ 2 hrs □ 3 hrs or more

---

6. Please list the electronic device(s) that the child uses at home, with the primary device first.

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________
5. ______________________________
6. ______________________________
7. ______________________________
8. ______________________________

7. **What activities does your child perform on the mobile device(s)? Check all that apply.**
   - ☐ Play games that are **app**-based
   - ☐ Play games that are **web**-based
   - ☐ Watch video clips (e.g. YouTube)
   - ☐ Watch shows or movies (e.g. Netflix)
   - ☐ Use instant messaging
   - ☐ Use texting
   - ☐ Use email
   - ☐ Browse the Internet
   - ☐ Listen to music (e.g., iTunes)
   - ☐ Use device's camera to take pictures
   - ☐ Use device's camera for video messaging (e.g. Facetime, Skype)
   - ☐ Post pictures (e.g. on social media)
   - ☐ Use online authoring tools (e.g., Google docs)
   - ☐ Other. Please specify ____

---

8. **Has your child used a comic book app before?**

☐ Yes ☐ No

If YES, please explain:

---

9. **Has your child had prior education about privacy or online safety?**

☐ Yes ☐ No

If YES, please explain:

---

10. **What house rules do you have for your children regarding device use and going online?**

    1) **I monitor my child's device use.**

       ☐ Always ☐ Sometimes ☐ Never

    2) **I have full access to my child's online accounts.**

       ☐ Always ☐ Sometimes ☐ Never

    3) **My child's account is linked to my account.**

       ☐ Always ☐ Sometimes ☐ Never

    4) **My child must ask for permission before downloading an app.**

       ☐ Always ☐ Sometimes ☐ Never

    5) **My child must ask for permission before going online.**

       ☐ Always ☐ Sometimes ☐ Never

    6) **My child must ask for permission before contacting other people online.**

       ☐ Always ☐ Sometimes ☐ Never

    7) **I prohibit the use of social media until my child is older.**

       ☐ Always ☐ Sometimes ☐ Never

    8) **I restrict my child's access to certain apps/services/resources.**

       ☐ Always ☐ Sometimes ☐ Never

    9) **I limit how much time my child can spend on the device.**

       ☐ Always ☐ Sometimes ☐ Never

    10) **I delete apps from my child's device if I don't think they are age-appropriate.**

       ☐ Always ☐ Sometimes ☐ Never

11) I check my child's browsing history.

☐ Always ☐ Sometimes ☐ Never

12) I use parental control tools.

☐ Always ☐ Sometimes ☐ Never

13) I check privacy settings on my child's device.

☐ Always ☐ Sometimes ☐ Never

14) I check what apps have access to on the device (e.g., location, camera).

☐ Always ☐ Sometimes ☐ Never

15) I deny access to device if my child misbehaves.

☐ Always ☐ Sometimes ☐ Never

16) I try to keep my technology knowledge up-to-date so I can monitor my child.

☐ Always ☐ Sometimes ☐ Never

17) My child uses safe-texting apps.

☐ Always ☐ Sometimes ☐ Never

18) I educate my child about online risks.

☐ Always ☐ Sometimes ☐ Never

19) Other. Please explain:

C.5: Parental Demographic Questionnaire

This information will be held completely confidential. (Please, do not put your name on this form!)

1. Age:

□ 18 – 24 Years

□ 25 – 29 Years

□ 30 – 34 Years

□ 35 – 39 Years

□ 40 – 44 Years

□ 45 – 49 Years

□ 50+

2. Gender:

□ Male

□ Female

3. Level of Education:

□ Some School but no diploma

□ High School Diploma

□ College Diploma

□ Bachelor Degree

□ Master Degree

□ PhD Degree

□ Other: ____

4. Current Profession: ____

C.6: Parental Pre-Evaluation Questionnaire

Please RANK from 1 to 5 the importance of these criteria in an educational app, where 1 is the most important, and 5 is the least important. Use each rank only once.

__________ **The comic book is fun for my child.**

__________ **The comic book is age-appropriate for my child.**

__________ **The comic book is easy-to-use for my child.**

__________ **The content of the comic book is educational for my child.**

__________ **The comic book is effective for my child as a learning tool.**

C.7: Parental Post-Evaluation Questionnaire

Please select or give the most accurate answer to each question below.

1. How fun was the comic book?

□	□	□	□	□
Very boring	Boring	Neither	Fun	Very fun

2. How age-appropriate was the comic book?

□	□	□	□	□
Very inappropriate	Inappropriate	Neither	Appropriate	Very appropriate

3. How easy to use was the comic book?

□	□	□	□	□
Very Difficult to use	Difficult to use	Neither	Easy to use	Very Easy to use

4. How educational was the comic book?

□	□	□	□	□
Very Non-Educational	Non-Educational	Neither	Educational	Very Educational

5. How effective was the comic book as a learning tool for children?

□	□	□	□	□
Ineffective	Ineffective	Neither	Effective	Very Effective

6. **How willing would you be to read the comic book again?**

☐	☐	☐	☐	☐
Very Reluctant	Reluctant	Neither	Willing	Very willing

7. **How willing would you be to recommend the comic book to your child?**

☐	☐	☐	☐	☐
Very Reluctant	Reluctant	Neither	Willing	Very willing

8. **How well did you and your child interact with the comic book?**

☐	☐	☐	☐	☐
Very poorly	Poorly	Neither	Well	Very well

9. **How well did the comic book facilitate conversations about privacy between you and your child?**

☐	☐	☐	☐	☐
Very poorly	Poorly	Neither	Well	Very well

10. **What did you like about the comic book?**

11. **What did you dislike about the comic book?**

12. **What would you add or change to the comic book? Please explain:**

C.8: Text Condition Copy

IS YOUR ONLINE PRIVACY JEOPARDIZED?

People's privacy is increasingly being jeopardized by images uploaded using smartphones. These images contain detailed metadata that can be used for identity theft or stalking!

Learn how to protect your own privacy as well as others.

Introduction

Nina: Hi, I'm agent Nina, and this is my partner Jack.

Jack: We've been fighting to protect users from "Hack", who has committed countless crimes against Internet users worldwide.

Nina: When given the opportunity, he may infect your computer with viruses and malware, steal your financial and personal information, disguise himself as someone you know and trust, and steal your identity to commit crimes against others.

Jack: Our mission is to pass on our knowledge about website security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.

Mobile Online Privacy - Understanding geo-tagging, and the risk of online tracking.

Jack takes a picture using his mobile phone of a little boy playing with a puppy and uploads the picture to social media. The little boy pats the puppy on the head and says: "Good boy Rufus!"

"I love using my phone to take pictures," said Jack. "Uploading them online is convenient and fun! But did you know you could be revealing sensitive location-based data to Hack about you, your family, or friends?"

"Pictures taken by most smartphones automatically attach location based data called geo-tagging," he continued. "Geo-tagging photos is a useful feature on the Internet, allowing people to share the location of experiences through their photos, such as where you took a picture of a sunset, an awesome event, or the location of that amazing restaurant you tried!"

"On the flip side", he cautioned, "there is a risk of online tracking with geo-tagged photos." Jack pulls out a picture of dreamy beach sunset, a lively concert photo, and a picture of a delicious-looking plate of sushi. Upon closer inspection, the three photos displayed the following information:

IMG_3857.jpg	IMG_2457.jpg	IMG_7584.jpg
Location: Cancún, Mexico	Location: Montreal, Canada	Location: Toronto, Canada
Date: December 21, 2013	Date: January 2, 2014	Date: March 11, 2014
Time: 5:10pm	Time: 8:56pm	Time: 7:17pm
Latitude: 21.1606° N	Latitude: 45.5000° N	Latitude: 43.7000° N
Longitude: 86.8475° W	Longitude: 73.5667° W	Longitude: 79.4000° W

“A picture’s worth a 1000 words,” Jack described. “The old saying is amplified with what we reveal through digital photos online today. Hack could easily obtain this data online through information extracted from pictures posted online using your phone, a process known as online tracking. Hack’s recent victim is Jane...”

Jane is an average woman with a family and kids. From Jane’s geo-tagged photos, the super villain hacker, Hack, was able to track what Jane is doing and where she went that day.

Before going to work, Jane walks the family pet, Rufus, and decides to upload a picture of her furry friend to Facebook with the comment: "Morning walk with Rufus!"

The photo of the dog could reveal the following information:

Time: 8:12 AM

Location: Near home

Pet’s Name: Rufus (Jane uses variations of her pet’s name for several of her password protected online accounts!)

Jane drops off her kids, Ashley and Chris, at school. Jane took a picture of the kids with their friends, Michael, Jess, and Mimi, and uploads it online with the message: "Ashley's first day of school!"

The photo of the kids could reveal the following information:

Time: 8:45 AM

Location: Riverbank Public School

Kids’ names: Not only did Jane reveal where her kids go to school; the picture also contains information about other kids they know.

Caution: Jane and her family leave the house around this time daily.

At work, Jane’s coworkers threw a surprise birthday party for Jane! A close co-worker tagged Jane in a photo she posted online. The photo generated 18 likes and 38 birthday related comments on Facebook.

The photo of the birthday party could reveal the following information:

Time: 11.03 AM

Location: Glendale ave. and Park St.

Jane’s birth date: Birth dates are often used for identity confirmation.

Caution: Even though Jane did not take the photo herself, being tagged in the photo compromised her privacy.

Jane met up with her best friend Rebecca for lunch, who is in town for a week., Jane often posts photos of food she loves online. She uploaded a photo of two vanilla milkshakes with the comment: “Girl time with Rebecca!”

The photo of the milkshake could reveal the following information:

Time: 12.25 PM

Location: Luna Cafe

Friend’s name and location: Jane revealed that her friend Rebecca is away from her own home.

Favorite foods: It turns out that “vanillamilkshake” is Jane’s banking password.

After work, Jane bought a new pair of flip-flops for her upcoming vacation to Mexico. She uploads a photo of her suitcase online with the comment: “Can’t wait for Mexico! All packed and ready to go!”

The photo of Jane’s suitcase and contents could reveal the following information:

Time: 5:56 PM

Location: Bank St. and River St.

Travel plans: Jane revealed that she is leaving town (no one is going to be home)

Travel info and credit card: Jane didn’t carefully check the content of the photo. Copies of her plane tickets and credit card are clearly visible.

In the evening, Jane took a picture of a chair she wanted to sell and posted it on Craigslist along with her contact information:

"Leather chair in great condition!" Contact Jane at 275-374-2654 or email jane49@email.com

The photo of the chair could reveal the following information:

Time: 10:48 PM

Location: Greenwood St. and Hazel St.

Home address: GPS coordinates of the photo revealed her home location.

Phone number and email: Jane included her phone number and email in her contact information, which could be seen by anyone!

“Location information is typically given as latitude and longitude coordinates”, said Nina. “Which can pinpoint the place where the photo was taken with a high degree of precision!” Jack added. “The GPS of smartphones can report location as accurately as 3 meters! That’s about the length of 3 baseball bats.”

“GPS coordinates are included with the image in the metadata tag, called EXIF. EXIF stands for Exchangeable Image File Format. Metadata information can be edited or filtered out with an “EXIF” editor (It’s a mobile app). Pictures edited this way can be free from geo-tagging information and can be posted online more safely.”

“Many mobile apps have the ability to use the phone’s camera directly. Take the time to understand the geo-tagging default settings of your apps and how the settings can be changed to stop attaching geo-tagging information to pictures.”

“Every smartphone has the geo-tagging feature automatically set on by default,” Nina continued. “It is recommended that you disable geo-tagging and enable it again only when needed.”

“Be also mindful of the contents of the images you post online,” cautioned Nina. You may unintentionally reveal personal information about others! These may include birth dates, addresses, phone numbers, and many other types of information! Don’t forget, user comments on photos may also contain personal information that can be used for identity theft or stalking!”

For example, Jane’s friend posted some comments on her social media on her birthday:

> “Happy birthday Jane! Have a great day!” Posted on January 25, at 9:17pm
>
> “Happy B-Day Jane! See you back on the 28th!” Posted on January 25, at 8:09pm
>
> “Have fun in Mexico!” Posted on January 25, at 6:23pm

“Help to protect your own privacy as well as others,” said Nina. “Hide your trail from Hack.”

THE END

Please complete the following review quiz:

Evaluate each statement carefully, and decide whether it is true or false.

1. Using my phone to upload photos is safe.

True False

A: False. Photos uploaded from your mobile device could reveal location and personal information.

---

2. Someone can track my location using the photos uploaded from my smartphone.

True False

A: True. Geo-tagged photos could reveal location information such as GPS coordinates, as well as other types of information, such as date and time. Pictures taken by most smartphones automatically attach location based data. This is called geo-tagging.

---

3. My location is used only for the GPS app on my smartphone.

True False

A: False. Many mobile apps have the ability to use the phone's camera. You should take some time to understand the geo-tagging default settings of these apps.

---

4. Location information can be extracted from images uploaded online by default.

True False

A: True. Every smartphone has the geo-tagging feature automatically set on by default. This information can be easily extracted by anyone.

---

5. I don’t need to take any action to protect my privacy while uploading pictures from my smartphone.

True False

A: False. It is not only your responsibility to protect your own privacy, but also respect the privacy of others when posting images. location information extracted from pictures posted online could lead to online tracking!

---

6. I need to change the settings on my smartphone to disable geo-location sharing.

True False

A: True. You should disable the geo-tagging feature on your smartphone and enable it again only when needed. Remember these setting are enabled by default, so you need to manually disable them.

Appendix D

Children's Privacy User Study Material

D.1: Interview Questions – Child

Q1. Do you use a phone, iPad, or iPod, or a Nintendo? If yes, what is it? Whose phone, iPad, or iPod, is it? Yours, mom, or dad, or your older brother(s), sister(s) or your friend's?

Q2. How often do you use it?

Q3. When do you use it?

Q4. How long? Is there a time limit?

Q5. Do you bring your phone, iPad, iPod, or Nintendo to school? Do your mom or dad says it's okay? What about your teachers?

Q6. What do you do with your phone, iPad, iPod, or Nintendo? Do you play games on it? If so, what kind of games?

Q7. Do you use it in class activities? Or do you use it to do your homework?

Q8. Who downloads or buys the apps? You, older brother/sister, other friends in class, your mom or dad? Who chooses which apps to get? How do you decide?

Q9. How often do you get a new app/game?

Q10. Do you have to ask mommy or daddy before you download or buy a game?

Q11. Does your mom or dad play any games with you?

Q12. Are they around when you play games or use your (phone/iPod/iPad/Nintendo)?

Q13. Do you chat with other kids/players online?

Q14. What apps/games do you use in order to chat with your friends/or other players?

Q15. Do you have your own account with a user id and a password? Or do you use mom's or dad's, or a brother or sister?

Q16. If so, I don’t want you to tell me your password, but I just want to know is it a hard to remember password or an easy to remember one? Do you share it with your friends or your mom, dad or any of your brothers or sisters?

Q17. Do you share information about yourself online?

Q18. Has anyone taught you rules for what you can and cannot do with the mobile device (ipad, ipod, phone)? What are they? Who taught you? Do you always follow these rules?

Q19. Do you know anything about privacy and security online? What should you do to make sure you’re safe?

D.2: Interview Questions - Parent

Q1. Does your child own a mobile device: phone, ipod, ipad, Nintendo? If a gaming device, then are they able to connect to the Internet or have access to other players online?

Q2. How does your child use the mobile device? What kind of activities do they perform on it?

Q3. Where does your child use the mobile device(s) most of the time? Home, school, elsewhere?

Q4. How many hours does your child use their mobile device(s) per day?

Q5. How many hours per day does your child spend online, whether on a mobile or a desktop computer?

Q6. Does your child download apps from their mobile device? If so, then who downloads them?

Q7 Who chooses which app to download? How do you decide?

Q8. Do you look at the app permissions before you download the game with/for your child?

Q9. Do you play any games with your child on the mobile device (phone/iPod/iPad/Nintendo)? What are they?

Q10. How many children's apps do you/your child download a week?

Q11. Does your child have their own account(s) online or do they use an existing account? If they have their own account(s), who helped them to create these accounts?

Q12. Do you know their user name and password? Do you know if they share it with anyone like their friends or siblings?

Q13. Does your child chat with other kids/players online?

Q14. Do you know which apps/games do they use in order to chat with their friends/or other players?

Q15. Do you know if they share information about themself online?

Q16. Does your child have rules for what they can and cannot do with the mobile device? What are they? Do they always follow these rules?

Q17. Does your child know anything about how to behave securely online and how to protect their privacy? If yes, then what do you think they know?

Q18. Have you spoken to your child about the risk of sharing too much of their private information online?

D.3: Demographic Questionnaire

This information will be held completely confidential. (Please, do not put your name on this form!)

1. Child's age ______________

2. Child's Gender:

☐ Male
☐ Female

3. Parent's Age:

☐ 18 – 24 Years
☐ 25 – 29 Years
☐ 30 – 34 Years
☐ 35 – 39 Years
☐ 40 – 44 Years
☐ 45 – 49 Years
☐ 50+

4. Parent's Gender:

☐ Male
☐ Female

5. Parent's Level of Education:

☐ Some School but no diploma
☐ High School Diploma
☐ College Diploma
☐ Bachelor Degree
☐ Master Degree
☐ PhD Degree
☐ Other: ____

6. Parent's Current Profession: ____

Appendix E

Cyberheroes User Study Material

E.1: Pre- and Post-Test Interview with Children

(The following questions were used twice, first as a pre-test, and second as a post-test.)

Privacy and Online privacy

1. What is “privacy”?
2. What could you do when you want privacy?
3. What could happen if you had no privacy?
4. What is “online privacy”?
5. What could you do when you want online privacy?
6. What could happen if you had no online privacy?
7. Have you learned about online privacy before from a parent or a teacher? What did you learn?

Personal Information:

1. What is personal information?
    a. Can you give me some examples?
2. You’re playing a game and it needs your phone number and birthday so that one of the characters can call you to say Happy Birthday… what would you do?

Talking to people online:

3. You’re playing a game and someone named Alex (or Ava) sends you a message. You don’t know Alex (or Ava), but he/she seems really nice and he sent you a funny picture…. What would you do? Why?

Location sharing:

4. You’re playing a game and someone named Evan (or Erin). You don’t know Evan (or Erin), but he/she seems really nice and wants to help you with your game. He/she asks you to meet him/her to discuss the game together, what would you do? Why?

Cyber-bullying:

5. You are talking to your friends online. One of them said something rude and mean to you, what would you do? Why?

Passwords:

6. Your best friend wants to borrow your password to email a funny picture to a friend that you both know, what would you do? Why?

Digital footprint:

7. If you posted something about yourself online like a picture, does deleting the picture erases it from the Internet? Why?

E.2: One-week Interview with Children

Online privacy

8. What is "online privacy"?
9. What could you do when you want online privacy?
10. What could happen if you had no online privacy?

Personal Information:

11. What is personal information?
    a. Can you give me some examples?
12. You're playing a game and it needs your name, address, and email so it can send you game tips… what would you do?

Talking to people online:

13. You're playing a game and someone named Ethan (or Eva) sends you a message. You don't know Ethan (or Eva), but he/she seems really nice and he sent you a funny video…. What would you do? Why?

Location sharing:

14. You're watching a funny puppy video on YouTube made by someone named Logan (or Laura). You don't know Logan (or Laura) but he/she seems really nice. He/she wants to show you the puppies and asks to meet you, what would you do? Why?

Cyber-bullying:

15. You are talking to your friends online. One of them is gossiping about the kids at school and said something rude and mean, what would you do? Why?

Passwords:

16. Your best friend wants to borrow your password to email a funny video to a friend that you both know, what would you do? Why?

Digital footprint:

17. If you posted something about yourself online like your game profile, does deleting the game account erases the profile from the Internet? Why?

Additional questions for the book-condition:

18. Can you tell me what the book you read last week was about?
19. Can you tell me what are the things you learned from the book?
20. What are the cyber-hero rules about
    - personal information
    - trust online
    - location
    - bullies
    - passwords

E.3: Children's Post-Evaluation Questionnaire

For each question, please circle the word that best describes your answer.

1. Would you read the How to be a Cyber-hero storybook again?

No	**Maybe**	**Yes**

2. How fun was the How to be a Cyber-hero storybook?

Very Boring	**Boring**	**Neither**	**Fun**	**Very Fun**

3. How easy was it to use the How to be a Cyber-hero storybook?

Very Hard	**Hard**	**Neither**	**Easy**	**Very Easy**

4. How well did you learn from the How to be a Cyber-hero storybook?

Very Bad	**Bad**	**Neither**	**Well**	**Very well**

5. How likeable were Ally and Bobby?

Very Dislikeable

Dislikeable

Neither

Likeable

Very Likable

---

6. How willing would you be to show the How to be a Cyber-hero storybook to other kids?

Very Unwilling

Unwilling

Neither

Willing

Very Willing

---

7. What did you like about the How to be a Cyber-hero storybook?

8. What did you dislike about the How to be a Cyber-hero storybook?

E.4: Children's Demographic Questionnaire (Completed by Parents)

Please select or give the most accurate answer to each question below.

1. What is your child's age?

☐ 6 yrs ☐ 7 yrs ☐ 8 yrs ☐ 9 yrs

---

2. What grade is your child in school?

☐ Grade 1 ☐ Grade 2 ☐ Grade 3 ☐ Other: __________

---

3. What is your child's gender?

☐ Male ☐ Female

---

4. How long does your child spend on mobile device(s) daily?

☐ 20min or less ☐ 40min or less ☐ 1 hr ☐ 2 hrs ☐ 3 hrs or more

---

5. How long does your child go online daily?

☐ 20min or less ☐ 40min or less ☐ 1 hr ☐ 2 hrs ☐ 3 hrs or more

---

6. Please list the electronic device(s) that the child uses at home, with the primary device first.

1. ______________________________ 5. ______________________________

2. ______________________________ 6. ______________________________

3. ______________________________ 7. ______________________________

4. ______________________________ 8. ______________________________

7. **What activities does your child perform on the mobile device(s)? Check all that apply.**
   - ☐ Play games that are **app**-based
   - ☐ Play games that are **web**-based
   - ☐ Watch video clips (e.g. YouTube)
   - ☐ Watch shows or movies (e.g. Netflix)
   - ☐ Use instant messaging
   - ☐ Use texting
   - ☐ Use email
   - ☐ Browse the Internet
   - ☐ Listen to music (e.g., iTunes)
   - ☐ Use device's camera to take pictures
   - ☐ Use device's camera for video messaging (e.g. Facetime, Skype)
   - ☐ Post pictures (e.g. on social media)
   - ☐ Use online authoring tools (e.g., Google docs)
   - ☐ Other. Please specify ____

---

8. **Has your child read an interactive e-book before?**

☐ Yes ☐ No

If YES, please explain:

---

9. **Has your child had prior education about privacy or online safety?**

☐ Yes ☐ No

If YES, please explain:

---

10. What house rules do you have for your children regarding device use and going online?

1) I monitor my child’s device use.

☐ Always ☐ Sometimes ☐ Never

2) I have full access to my child’s online accounts.

☐ Always ☐ Sometimes ☐ Never

3) My child’s account is linked to my account.

☐ Always ☐ Sometimes ☐ Never

4) My child must ask for permission before downloading an app.

☐ Always ☐ Sometimes ☐ Never

5) My child must ask for permission before going online.

☐ Always ☐ Sometimes ☐ Never

6) My child must ask for permission before contacting other people online.

☐ Always ☐ Sometimes ☐ Never

7) I prohibit the use of social media until my child is older.

☐ Always ☐ Sometimes ☐ Never

8) I restrict my child’s access to certain apps/services/resources.

☐ Always ☐ Sometimes ☐ Never

9) I limit how much time my child can spend on the device.

☐ Always ☐ Sometimes ☐ Never

10) I delete apps from my child’s device if I don’t think they are age-appropriate.

☐ Always ☐ Sometimes ☐ Never

11) I check my child’s browsing history.

☐ Always ☐ Sometimes ☐ Never

12) I use parental control tools.

☐ Always ☐ Sometimes ☐ Never

13) I check privacy settings on my child’s device.

☐ Always ☐ Sometimes ☐ Never

14) I check what apps have access to on the device (e.g., location, camera).

☐ Always ☐ Sometimes ☐ Never

15) I deny access to device if my child misbehaves.

☐ Always ☐ Sometimes ☐ Never

16) I try to keep my technology knowledge up-to-date so I can monitor my child.

☐ Always ☐ Sometimes ☐ Never

17) My child uses safe-texting apps.

☐ Always ☐ Sometimes ☐ Never

18) I educate my child about online risks.

☐ Always ☐ Sometimes ☐ Never

19) Other. Please explain:

E.5: Parental Demographic Questionnaire

This information will be held completely confidential. (Please, do not put your name on this form!)

1. Age:

☐ 18 – 24 Years

☐ 25 – 29 Years

☐ 30 – 34 Years

☐ 35 – 39 Years

☐ 40 – 44 Years

☐ 45 – 49 Years

☐ 50+

2. Gender:

☐ Male

☐ Female

3. Level of Education:

☐ Some School but no diploma

☐ High School Diploma

☐ College Diploma

☐ Bachelor Degree

☐ Master Degree

☐ PhD Degree

☐ Other: ____

4. Current Profession: ____

E.6: Parental Pre-Evaluation Questionnaire

Please evaluate how important each criterion is to you in an educational interactive children's storybook about privacy.

1. The interactive storybook is fun for my child:

□	□	□	□	□
Very important	Important	Neither	Unimportant	Very unimportant

2. The interactive storybook is age-appropriate for my child:

□	□	□	□	□
Very important	Important	Neither	Unimportant	Very unimportant

3. The interactive storybook is easy-to-use for my child:

□	□	□	□	□
Very important	Important	Neither	Unimportant	Very unimportant

4. The content of interactive storybook is educational for my child:

□	□	□	□	□
Very important	Important	Neither	Unimportant	Very unimportant

5. The interactive storybook is effective for my child as a learning tool:

□	□	□	□	□
Very important	Important	Neither	Unimportant	Very unimportant

E.7: Parental Post-Evaluation Questionnaire

Please select or give the most accurate answer to each question below.

1. How fun was the interactive storybook?

□	□	□	□	□
Very boring	Boring	Neither	Fun	Very fun

2. How age-appropriate was the interactive storybook?

□	□	□	□	□
Very inappropriate	Inappropriate	Neither	Appropriate	Very appropriate

3. How easy to use was the interactive storybook?

□	□	□	□	□
Very Difficult to use	Difficult to use	Neither	Easy to use	Very Easy to use

4. How educational was the interactive storybook?

□	□	□	□	□
Very Non-Educational	Non-Educational	Neither	Educational	Very Educational

5. How effective was the interactive storybook as a learning tool for children?

□	□	□	□	□
Ineffective	Ineffective	Neither	Effective	Very Effective

6. How willing would you be to read the interactive storybook again with your child?

□ Very Reluctant   □ Reluctant   □ Neither   □ Willing   □ Very willing

---

7. How willing would you be to use the interactive storybook to teach your child about privacy?

□ Very Reluctant   □ Reluctant   □ Neither   □ Willing   □ Very willing

---

8. How well did you and your child interact with the storybook?

□ Very poorly   □ Poorly   □ Neither   □ Well   □ Very well

---

9. How well did the interactive storybook facilitate conversations about privacy between you and your child?

□ Very poorly   □ Poorly   □ Neither   □ Well   □ Very well

---

10. What did you like about the interactive storybook?

11. What did you dislike about the interactive storybook?

12. What would you add or change to the interactive storybook? Please explain:

E.8: Text Condition Copy

Cyberheroes

Psssst! Want to know a secret? Seven year-old Ally Sanders and her brother nine-year-old Bobby Sanders are cyberheroes in disguise! Cyberheroes have cyberpowers. They must keep their identities a secret when they go on the Internet. That's the number one rule.

One day, Ally and Bobby stopped practicing their cyberpowers…and forgot all the cyberhero rules! Bobby forgot the power of Cyber-Disguise, and gave his personal information to sign up for an online game. It got collected by cybervillains.

Bobby's personal information:

- Name (Bobby Sanders)
- Address (68 Sunny Lane)
- Phone number (363-297-5799)
- Birthday (Oct. 21)
- Age (9)
- School (Three Oaks Primary)

Remember, the first cyberhero rule is to never, ever provide personal information to anyone on the Internet without asking a grownup first.

Ally forgot the power of Cyber-Xray-Vision, and was fooled by other people's disguises on the internet.

Ally talked to:

- Aunt Peggy (42 years old)
- Alex (8 years old). He is actually Mr. R (47 years old).
- Kitty (age unknown). She is actually Erin (36 years old).
- Cousin Tia (9 years old).

The second cyberhero rule is to be careful of who you trust online. Not everyone is who they say they are on the Internet!

Bobby forgot the power of Cyber-Invisibility, and shared his locations (at home, at school, at the secret hideout). The third cyberhero rule is to never reveal where you are, especially to strangers.

Ally forgot the power of Cyber-Empathy, and said mean things (gossip, insults, and teasing) to a friend on internet chat. The fourth cyberhero rule is to be kind! If someone says something rude and mean, don't respond. Walk away, and talk to your parents.

Lastly, they both told other people their password (Heroes4Ever) to access their secret files! The fifth cyberhero rule is to always keep passwords a secret!

Oh my, everyone knows who they are! Their digital trail is all over the internet! Bobby and Ally didn't care. "We could just delete everything" they thought. They tried to erase their digital trail, but the tracks wouldn't disappear. They are on the internet forever and ever!

Bobby and Ally are very sad. They lost their privacy online and could not play safely. They want their cyberpowers back. But how? Then, they realized that all the children could have cyberpowers. You only have to learn and practice them.

Cyber-Disguise - never, ever provide your personal information to anyone.

Cyber-X-Ray - be careful of who you trust online.

Cyber-Invisibility - never reveal where you are, especially to strangers.

Cyber-empathy – be kind to others.

Cyber-password - always keep your passwords to yourself.

So put on your disguises, practice your cyberpowers, and get ready to become cyberheroes!

The end.