Cybersecurity Comic: An Image Change to "Cool Cybersecurity" Findings and Challenges to Raise Children's Security Awareness

Jennifer Friedauer
Ruhr-University Bochum

Harunobu Yagi
Central Japan Railway Company

Nissy Sombatruang
National Institute of Information and Communications Technology

Youki Kadobayashi
Nara Institute of Science and Technology

Daisuke Miyamoto
The University of Tokyo

Akira Fujita
National Institute of Information and Communications Technology

Abstract

The market for security awareness products is rapidly growing, already larger than 1 billion USD. Despite these investments the number of threats and successful attacks is increasing. Most awareness vendors focus their products on organisations and adult users. In this work we propose an approach to raise security awareness by carrying cybersecurity scenarios to children at school. We developed a comic in order to evoke children's interest in cybersecurity and tested the impact of our comic by conducting an online survey at 3 japanese elementary schools. The survey was answered before reading, directly after reading and 1 week after reading the comic. N=130 pupils took part in all three questionnaires. This work includes a description of our survey procedure and a report of our preliminary quantitative and qualitative results on the children's level of cybersecurity understanding, if their perception of cybersecurity is positive, and if they are interested in cybersecurity after reading the comic. Our results show a need for discourse after reading the comic, but it has high potential to evoke children's interest in the field of cybersecurity. In our study cybersecurity terms are recalled, but children found it difficult to describe them. Our findings can be helpful in developing material that evokes the interest of young children in cybersecurity as a field that can be explored.

1 Introduction

While cybersecurity threats are increasing, there are many areas of conflict. One of these areas is the question about responsibility. On the one hand there is the conflict that individuals often perceive security as something that should be done by experts and on the other hand cybersecurity experts often blame the user for their behaviour [7]. Menges et al. (2021) e.g. found the relationship between cybersecurity staff and employees dysfunctional. [7] Structures make it difficult to see what is being protected and only the occurrence of incidents stands out. This creates an overall negative image of cybersecurity. This negative image is built by negative communication and negative language used when talking about cybersecurity. [7] There are negative feelings that individual users have towards cybersecurity experts and negative feelings that cybersecurity experts have towards individual users [7]. This negative image might keep children away from cybersecurity as a topic that should be part of their daily lives. It is necessary to improve the image of cybersecurity on many levels and especially appeal to the younger generation that cybersecurity is something worth thinking and asking questions about.

Various methods are used to create awareness of different topics in education contexts. In this work we will present preliminary results of a project that aims to make cybersecurity a topic in children's daily discourse. We developed a Cybersecurity Manga (japanese comic) and conducted an online survey at 3 elementary schools in Chiba, Japan. The idea of the comic is that it is ongoing and will become a series with growing content. One advantage of a series is that the quality can develop over time if its content is evaluated.

Our main interest for this research was to find out if our comic increases...

RQ1 ...children's level of understanding of cybersecurity?
RQ2 ...children's positive perception about cybersecurity?
RQ3 ...children's interest in the field of cybersecurity?
RQ4 ...children's interest in choosing future career in the field of cybersecurity?

We start by explaining *security awareness*, review existing literature on children's security awareness and give an overview on their challenges and findings. We then describe our study procedure and the questionnaires we used as instruments to collect feedback from the children regarding our

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, M.A., USA.

comic. Our report will focus on advantages and challenges we found during our quantitative and qualitative analysis, the feedback we received and our future work decisions. We will not present our results on RQ 4 due to page limitations.

2 Background on Children's Cybersecurity Awareness

Security Awareness Security Awareness "is not training. The purpose of awareness presentations is simply to focus attention on security." [11] Awareness material should allow individuals to recognize IT security when they come across situations, problems or concerns that require awareness and appropriate action [11]. Awareness material is made for sensitizing. Appropriate action would be secure behaviour. *Secure Behaviour* requires not only awareness but information and an understanding of what secure behaviour is. [4] In addition it needs practise to gain experience. Prior experiences as well as positive emotions and feelings towards a task or topic strongly impact future behaviour and self-efficacy beliefs - the belief in one's own abilities and success [1].

Tools and Interventions to raise Children's Security Awareness There is a growing market for security awareness products [4]. Awareness material for or even research on privacy or security concerns of the elderly, teens and children is still a niche [5]. In this work we focus on our experts of tomorrow: Children. Tools and interventions for children to get insights into cybersecurity issues have been a topic of interest during the past few years. Giannakas et al. (2016) evaluated a game called CyberAware to teach fundamentals of internet safety and device protection before and after playing it with 6th grade children (n=43). The evaluation was mainly based on the usability of the app itself. Key findings of their work regarding the tool were, that ① **the kids were unhappy with the amount of reading** [3]. Results regarding the understanding of cybersecurity showed that it improved after playing the game. [3] Zhang-Kennedy and Chiasson (2016) developed an interactive e-book for kids on cybersecurity [6]. The effectiveness of this e-book was evaluated by comparing two studies. The first study was carried out by Zhang-Kennedy and Chiasson (2016) in the US (n=22) [6] and the second one carried out by Rouli (2021) in Canada (n=15) [8]. In both studies a pair, child and parent, participated. [8] The canadian study showed that ② **cybersecurity knowledge increased after reading** the e-book in both studies. Further result of the study in 2021 was that there were ③ **higher expectations and a desire for explanations** and ④ **"for effective narrative with well-developed plot and good character development"** [8]. Pencheva et.al. (2020) did a study based on workshops with teachers on the topic IT security. They found that ⑤ **teachers, parents but also peers are key contacts to motivate and strengthen dialogue and interests in the topic** [9].

Comics to raise Security Awareness - Hypothesis and Expectations With our comic we aim to address some of the challenges outlined by the previous studies. We want to build up interesting characters who experience a well-developed plot. For this purpose we choose the format of an ongoing comic series.

- H1 Children's level of understanding of cybersecurity increases after reading the comic
- H2 Children feel more positive toward cybersecurity after reading the comic
- H3 Children are interested in the field of cybersecurity after reading the comic

3 Methodology

3.1 Cybersecurity MANGA for Children

The comic was developed at ICSCoE in Japan. Artist and researchers worked close together, to create a full storyline for the comic, with individual characters who each have their own personalities. This study was carried out with the Japanese version. The comic was made publicly available online in Japanese, English and German language.[1]

Overall, the story takes place in a city called Cyberspace. The characters who live in Cyberspace are technical devices who interact with each other during their daily life [12]. The technical devices are displayed as human characters of which most of them care about their security. Symbols of care are fashion accessories or for example a dog-like pet that accompanies the character and implies an antivirus program [12]. The main characters of the story experience situations like an encounter with an unprotected device or becoming victim of a phishing attack. They are confronted with malware and ransomware attacks and cannot be protected by their pet companions [12]. The characters need help to get out of these critical situations. Threats and villains are personified as different creatures who in the end want to take over the city.

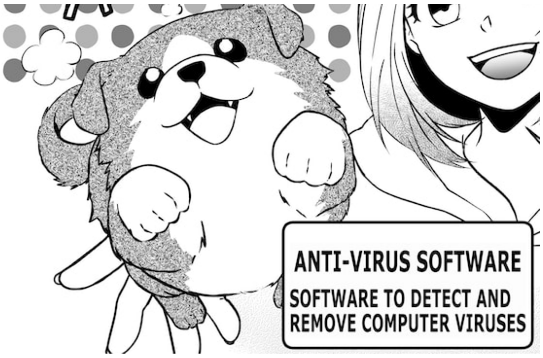

Figure 1: Antivirus character and description in the comic.

[1]The English version of the comic can be found here: https://tapas.io/series/EVERYDAY-ZERODAY/info

Whenever a security term occurs in the comic it is explained in an additional text box. Figure 1 shows an example: Antivirus is explained as *"software to detect and remove computer viruses"* [12].

3.2 Evaluation Procedure

Recruiting and Sample To get first impressions on our comic we managed to recruit pupils at 3 elementary schools at Chiba Prefecture, Japan and received permission of the school's authorities, teachers and the parents of the children to carry out our study. The majority of the children was in 6th grade (average age = 12), see Table1.

Ethics None of our main institutions (Faculty for Computer Science at Ruhr-University Bochum and the ICSCoE) has an internal IRB. Our study procedure follows the Ethical Principles and Guidelines for the Protection of Human Subjects of Research of the Belmont report [2] and we are in detailed contact with the Data Protection Officers at Ruhr-University Bochum who give us feedback regarding our ethics documents for the ongoing project. We followed data protection policies and provided a study description including data handling and consent forms to the schools and the parents before the study began. The researchers visited the schools to explain the study purpose and the procedure. All parties were informed that they could terminate participating in the study at any time without any consequences.

Procedure When the researchers visited the schools to explain the study purpose and the procedure they handed a sheet of paper to the teachers with the instructions. The teachers handed out the sheets in class. The material was handed out to 500 children. On the sheet were four QR codes that lead to the different tasks:

- QR Code 1 - access to the before reading questionnaire
- QR Code 2 - access for reading the comic
- QR Code 3 - access for the after reading questionnaire
- QR Code 4 - access to the week after reading questionnaire

3.3 Survey Contents

Demographic Questions In the before reading questionnaire we added questions about demographic information like the grade at school and gender. We additionally asked for the familiarity with reading Manga and how often they use technical devices (Options were: *every day, a few times a week, a few times a month, a few times a year, never*).

Questionnaire Every participating child got an ID they had to type in. Via this ID, the questionnaires could be assigned to each other without using the children's names. The first question that was part of all three questionnaires was **How do you feel about cybersecurity** (RQ2). (Options were: *I think it's very cool, I think it's cool, I feel neutral about it, I don't think it's cool. I don't think it's cool at all, I don't know.*) With this item we tried to measure the first impressions our comic makes and if the children see cybersecurity as some interesting, attractive topic and something worth spending time with.

To measure children's understanding about cybersecurity terms that are used in the comic we asked them to **select the words they know and which they identify as a cybersecurity word.** (RQ1) (Options were: *Anti-virus software, terminal quarantine, access monitoring, digital forensics, access control, firewall, C&C server, malware, ransomware, data encryption, secure communication, I don't know*). A follow up question was a free text field in which the children had to describe the selected words.

To measure whether or not the field becomes more interesting (RQ3), we evaluated the additional comments and suggestions the children left in a free text field.

3.4 Data Analysis

Qualitative questionnaire data Our qualitative data from the questionnaire will be the comments and descriptions the children made in the free text fields, for H1 and H3. We analysed the statements in MAXQDA to gather information on feedback regarding the comic and regarding our hypothesis if the children show any interest, emotions or insecurity towards our material. We used both inductive and deductive approach in the software MAXQDA for data analysis [10].

These findings are essential for developing our study design and in a further step to improve our material for future work.

Quantitative questionnaire data We present first results of our descriptive analysis from our questionnaires. Originally the number of responses differed from n=172 before reading, n=157 after reading and n=133 one week after reading. For our statistical analysis we only considered the responses of the children who took part in all three questionnaires (n=130), see also Table1.

Table 1: Overview of those children who completed all three questionnaires (before reading, after reading and 1 week after reading)

Children who completed all questionnaires	N = 130
Sex	
Female	50
Male	71
No answer	48
Grade	
6th	130

4 Preliminary Results: Opportunities, Challenges and Limitations

In this section we present our findings regarding our research hypothesis with a special focus on opportunities and methodological challenges. ① **we did in general not receive comments regarding the amount of reading**.

② **Childrens level of understanding of cybersecurity was measured in form of a knowledge recall.** Directly after reading the children recognized the cybersecurity words in our questionnaire and marked them as known words more often. *Example:* Before reading the most known word by 33 of the 130 children (25%) was the *Antivirus Software*. The other terms were all known by less than 15 % of the children. After reading 89 (68 %) of the children recognized the word *Antivirus Software*. 1 week after reading 67 % of the children still recognised this term. Our Results regarding children's understanding [H1] are limited because we only have quantitative data about whether they recall a term - understanding is more than that. The *qualitative results* show that children did not make use of our free text field the way we asked them to and that they did not describe what they think these cybersecurity terms mean. On the other hand children commented that "[they've] learned from the comic"(7 Comments) Figure2.

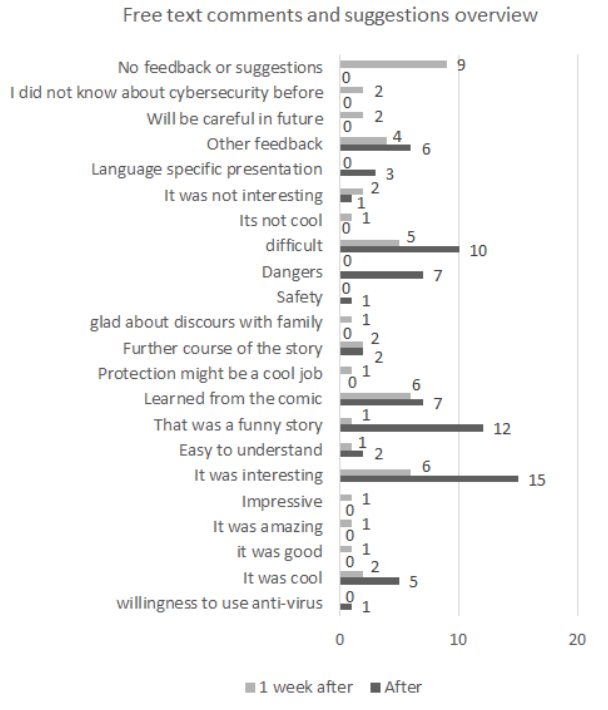

Figure 2: Quanlitative results from our comments and suggestions free text field

Childrens feelings toward cybersecurity [H2] Regarding children's ③ **expectations and a desire for explanations** we found that our material seems to be difficult to understand. 10 comments on difficulty and 3 on language specific presentation led us to this assumption. Statements on difficulties were for example that "the manga was a little bit confusing" or "it would be easier [...] to understand if the language of cyber security were made simpler". Figure2 ⑤ **We conclude that there is a need for discourse of the comic after reading** but we can definitely see it as an opportunity that children seem to ask questions and want to learn more about the topic. Our quantitative results show that the number of children who think that cybersecurity is a *cool* or *very cool* topic increased from 47 (36 %) before reading to 79 (61 %) after reading. In Figure2 we see that it left positive impressions like: it was "amazing"(1 comment), "good"(1 comment), "cool"(5 comments), "funny"(12 comments) or "interesting"(15 comments). Our results additionally show that ④ **children are more interested in the topic after reading and that they liked our story and plot** [H3]. Comments like "I am interested in continuing the story of the manga" or "It was very interesting. I would like to see the rest of the story" lead us to the assumption that this comic format might have potential to evoke interest in the field of cybersecurity.

5 Future Work

We found out that the majority of the comments regarding impressions, interest and difficulties are made directly after reading the comic. In addition, the overall amount of comments is bigger directly after reading the comic. Our future work plan is to further investigate children's understanding and experiences of cybersecurity to improve our study material and procedure. In the planned study we will directly create a discourse after reading the material, let the children ask their questions in class and talk about their experiences with our comic and the cybersecurity scenarios in the story. We hope that we can find out more about what children take home from reading our material, what was difficult to understand and if our comic strengthens self-efficacy beliefs of children in their own abilities to safely interact with technical devices [1] [5]. It is still an open question if the children are able to do the transfer from a created universe to their own life. Furthermore, we as security experts have to make cybersecurity scenarios, the communication about it [7] and term descriptions easier to understand for children and those we want to address and educate.

References

[1] Albert Bandura and Nancy E. Adams. Analysis of self-efficacy theory of behavioral change. *Cognitive Therapy and Research*, 1(4):287–310, 1977.

[2] National Commission for the Proptection of Human Subjects of Biomedical and Behavioral Research. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. [Bethesda, Md.]: The Commission, 1978.

[3] Filippos Giannakas, Georgios Kambourakis, Andreas Papasalouros, and Stefanos Gritzalis. Security education and awareness for k-6 going mobile. *International Journal of Interactive Mobile Technologies (iJIM)*, 10(2):41, 2016.

[4] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. "taking out the trash": Why security behavior change requires intentional forgetting. 2021.

[5] Reza Ghaiumy Anaraky; Marten Risius; Bart P. Knijnenburg. The Effects of Digital Literacy, Privacy Self-efficacy, and Privacy Concerns in Young and Older Adults' Privacy Decisions. In *6th Workshop on Technology and Consumer Protection*, ConPro '22, Virtual Conference, May 2022. IEEE.

[6] Leah Zhang-Kennedy and Sonia Chiasson. Cyberheroes: An interactive ebook for improving children's online privacy. *Proceedings of the 31st International BCS Human Computer Interaction Conference (HCI 2017)*, 2017.

[7] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, and Imogen Verret. Why it security needs therapy. In *Computer Security. ESORICS 2021 International Workshops*, pages 335–356, Cham, 2022. Springer International Publishing.

[8] My-Linh T. Rouil. *A Comparative Study in the Effectiveness of Interactive E-books to Teach Children Online Privacy and Security*. 2021.

[9] Denny Pencheva, Joseph Hallett, and Awais Rashid. Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, 18:68–74, 2020.

[10] Stefan Rädiker and Udo Kuckartz. *Focused Analysis of Qualitative Interviews with MAXQDA*. MAXQDA Press, 1 edition, 2020.

[11] M. Wilson and J. Hash. *Building an Information Technology Security Awareness and Training Program: NIST Special Publication 800-50*. 2003.

[12] Harunobu YAGI and Manga artist sohsuke. Everyday zeroday. https://tapas.io/series/EVERYDAY-ZERODAY/info, 2021. Accessed: 2022-05-05.