Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Enhancing Cybersecurity Resilience in African Children Through Culturally Tailored Comics

Jema David Ndibwile

jndibwil@andrew.cmu.edu

Carnegie Mellon University https://orcid.org/0000-0002-7962-2237

Fidelis Ayite

Carnegie Mellon University

Adeline Ishimwe Musonera

Carnegie Mellon University

Sabine Gisagara

Carnegie Mellon University

Rehema Mpinganzima

Carnegie Mellon University

Youki Kadobayashi

Nara Institute of Science and Technology

Research Article

Keywords: Cybersecurity, Culturally Relevant Comics, Digital Literacy, Preteens, Education

Posted Date: November 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11659045/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Enhancing Cybersecurity Resilience in African Children Through Culturally Tailored Comics

Jema David Ndibwile[1,2*], Fidelis Ephraim Ayite[1], Adeline Musonera Ishimwe[1], Sabine Gisagara[1], Rehema Mpinganzima[1], Youki Kadobayashi[2]

[1*]CyLab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, USA.
[2]Carnegie Mellon University Africa, Kigali, Rwanda.
[2]Laboratory for Cyber-Resilience, Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma, 630-0101, Japan.

*Corresponding author(s). E-mail(s): jeman@cmu.edu;
Contributing authors: fayite@alumni.cmu.edu;
aishimwe@alumni.cmu.edu; sgisagar@alumni.cmu.edu;
rmpingan@alumni.cmu.edu; youki-k@is.naist.jp;

Abstract

This study assesses how well a culturally appropriate comic book intervention increases preteen knowledge of cybersecurity between the ages of 10 and 13. The comic book group and the traditional notes group were randomly assigned to 300 participants from five Rwandan primary schools. From well-resourced private schools to under-resourced public and refugee camp schools, the schools represented a variety of socioeconomic backgrounds. Cybersecurity knowledge was assessed before and after the intervention and the results were analyzed using paired sample t-tests. With t statistics ranging from 2.14 to 7.74 and p-values ¡ 0.05, the comic book group showed significant improvements in all schools. In particular, the post-test scores in one of the schools, which is public and located in a rural location with few resources, improved by 75%. The feedback of the students showed strong levels of involvement, with 90% praising the African cultural characteristics and 95% finding the stories relatable. These results imply that, regardless of preteen socioeconomic status, culturally appropriate instructional resources can successfully raise awareness of cybersecurity.

Keywords: Cybersecurity, Culturally Relevant Comics, Digital Literacy, Preteens, Education

1 Introduction and Background

Comprehensive cybersecurity education is more important now than ever in our hyper-connected society, especially for African children and those living in rural or refugee camps. Due to the rapid embrace of digital technology on the continent, Africa's silicon savannahs are thriving at a time when smartphones make development more accessible than ever. But there are also unprecedented risks linked to this development in the digital domain, particularly for younger users who are unfamiliar with the reality of the digital age. The current study 'Enhancing Cybersecurity Resilience in African Children Through Culturally Tailored Comics' focuses on creating educational materials that are specifically suited to the cultural contexts in which African children are growing up in order to address these issues. Using the best practices of global initiatives that have been working to improve digital literacy and security among young Africans, with this research, we hope to contribute to a safer online landscape for our youth.

1.1 Cybersecurity Challenges in Africa

With the increase in the use of digital technology in daily life, it has become even more important that cybersecurity education reaches underserved populations worldwide, such as African pre-teens and those living in rural communities or refugee camps. The rapid adoption of the Internet in Africa, along with the surge in smartphone use, has resulted in an open digital realm that is mainly risky. According to a recent survey by the DQ Institute (2023), around 70% of children and adolescents aged 8 to 18 years worldwide have experienced at least one form of cyber risk in the past year, prompting experts to describe the situation as a 'cyberpandemic' [1]. In the African context, this figure is equally concerning. For example, in South Africa, 67% of children reported facing at least one cyber threat in the year 2022 [2]. The COSI report also shows that children in emerging ICT regions such as Africa are 1.3 times more likely to encounter cyber risks than those in advanced ICT countries, due to factors such as limited digital literacy and weak online safety policies [3].

Gaining a greater understanding of cybersecurity is necessary to build resilience to online threats. Unfortunately, there are often not enough educational resources available, particularly for people without access to technology or formal education. Traditional training methods tend to overlook cultural relevance, making it harder for beginners and younger users to understand core concepts. Furthermore, the absence of tailored academic content poses a major challenge in effectively teaching key topics such as online safety, digital privacy, and responsible internet use [4].

1.2 The Role and Need for Culturally Tailored Cybersecurity Education

Despite the continued global pursuit of improving cybersecurity education, there is still a vast scarcity of education materials that are developed specifically for African youth and underserved communities. There are many initiatives already in place that do not take into account the contexts and cultures that drive learning and this arguably

weakens the quality of educational initiatives and enhances the digital divide. This neglect places vulnerable groups at increased risk against cyber-harms.

It is important to make instructional resources culturally appropriate to increase understanding of complex topics. Studies show that culturally relevant strategies increase student attention and perseverance [5]. This method recognizes how students' cultural backgrounds serve as learning bridges in developing curriculum that relates to students' lived experiences, which helps to improve the meaning and impact of education. Culturally appropriate materials can enhance understanding and retention of memory; therefore, using culturally appropriate information can assist learners to understand cybersecurity issues.

Culturally appropriate resources, such as comic books, can be useful in the African context when trying to convey complicated cybersecurity ideas. The integration of informational text and visual narratives has been shown to promote understanding and engagement with younger audiences in comic book formats [6]. To this end, Mayer (2002) stated in his Multimedia Principle that students learn better with words and pictures together as opposed to just words [7]. He noted that when words and pictures were presented to students, both verbal and pictorial mental models can be constructed, and students can make links between the two. However, with just words, students can create a verbal mental model but are less likely to create a pictorial mental model and even less likely to make links between their two mental models.

In addition, including aspects of African culture in these stories provides a richness of learning experiences for students and allows readers to gain a deeper understanding of the cybersecurity challenges and solutions that are relevant to their daily lives.

To meet these challenges, it is vital to collaboratively create educational resources that reflect the cultural norms of African communities. It is the responsibility of educators to provide empowering and culturally relevant material that allows learners to feel connected to the content, even when they are in a potentially vulnerable situation. Creating a strong cybersecurity culture means identifying all types of learners who, through social learning, will move beyond rigid teaching methods and begin to understand the value of cultural and contextual elements in digital education as well. This will allow learners to be equipped, enabled, and empowered to proceed and thrive in their digital environment.

1.3 Comparative Insights from Global Initiatives

Learning from best practices of successful educational resources can help provide content guidance. Many countries have introduced new programs for the education of children and young people in cyberspace, and many of these can provide examples for Africa.

Japan: The National Institute of Information and Communications Technology (NICT) and Information-Technology Promotion Agency (IPA) were responsible for an elaborate program of educating the public about cyberspace security that included accessibility and engagement methods. It brought together workshops that provided interactional and visual content focused on children, young people and young adults [8]. Such best practices can help reflect on the best processes for developing materials that are contextually appropriate in Africa.

United States: The NICE has developed a variety of cybersecurity materials, including some materials for K–12 learners. One program, CyberPatriot, is a youth cyber education program backed by the Air Force Association, and by simulating cyber defense tournaments teaches young people useful skills [9].

United Kingdom: The National Cyber Security Center (NCSC) has a selection of key cyber security education programs for young people. One such program is CyberFirst, which is a national initiative to engage young people in tournaments and events and also a summer school so that the next generation can learn about essential cyber security. The NCSC also supports teachers by providing educational resources, such as lesson plans, to assist in embedding cyber education in the classroom [10].

Australia: The Stay Smart Online program - an initiative of the Australian Government - has resources and activities for young people on how to stay safe online. The program seeks to develop young people's cybersecurity awareness from an early age to improve safety when engaging with digital environments, it contains gamified activities and interactive modules to educate young people about various topics of cybersecurity. The part of the Australian Computing Academy also has cybersecurity challenges and learning modules that are applied as part of their Digital Technologies curriculum [11].

Estonia: Estonia is a modern country with contemporary digital infrastructures and e-Governance, and it has developed cybersecurity education as part of a national security policy. CyberOlympics was designed as a competitive event to raise student awareness about ethical dilemmas and possible cybersecurity issues by providing challenges and contests that could encourage, explore, and amplify the practical realm of their knowledge in the domain. Estonia has embedded cybersecurity in the national curriculum, using cybersecurity as a complementary teaching tool in comprehensive school education on digital literacy and digital security [12].

1.4 Japanese Inspiration for Manga Comics

As we work toward engagement, developing successful approaches for fostering cybersecurity education for Africa, we begin in a region where we are most comfortable, East Africa, specifically Rwanda. As observed in Japan and their successful approaches including the creative use of manga comic representations, we see the possibility of a similar approach to suit local cultures. We have a vision of continuing these efforts in other African countries and for the entire continent to benefit from the growth of cyber security professionals through digital security education.

In Japan, cybersecurity education starts and evolves thoughtfully, starting with elementary school students aged 7 to 12. In elementary schools, learners are first introduced to concepts. Through the use of manga, students are introduced to basic practices such as password authentication and the possible implications of leaking personally identifiable information through relatable figures who encounter relatable challenges in the digital realm. What makes reading impactful, compelling, and realistic are stories that contextualize education—and the apprehension often associated with it—through relatability [13].

As students advance to secondary school, aged 13 to 15, their understanding of cybersecurity deepens. At this stage, manga continues to play a significant role. The

narratives evolve to cover the risks associated with private information leaks and the basics of information protection through coding. The visual and narrative elements of manga facilitate a more deep understanding of these issues, encouraging students to apply their knowledge practically and responsibly [14].

In upper secondary school, for students aged 16 to 18, the focus shifts to more complex cybersecurity concepts. Here, manga explores advanced topics such as the implementation of comprehensive security plans and responses to network attacks. The sophisticated plots of these comics help students understand and apply proactive security measures, preparing them for real world challenges [15].

Japan's success in the manga-based educational strategy demonstrates potential for East Africa. However, it is critical to apply some local cultural aspects to this model. East Africa has a long history of visual storytelling, and the use of local artistic styles and themes would allow learners to better connect educational comics to cybersecurity concepts. Incorporating culturally relevant stories using local artists and storytellers would add to the richness of these educational genres.

In addition to local artists and storytellers, it is also important to include local community stakeholders throughout the development. Hearing from educators, parents, and students would help provide assurance that the comics are responding to legitimate community issues and needs. At the same time, it is important to strengthen the outreach and logistics needed to deliver these comic magazines to local schools and communities. Partnering with schools or using digital platforms can significantly improve access and distribution.

Through a localized adaptation of Japan's manga-based approach, East Africa has the tools to create a meaningful and contextualized cybersecurity pedagogy. The goal of this idea is not only to improve students' understandings of cybersecurity in East Africa, but also to improve the safety and experience of ushers in that space by combining a contextualized approach to good pedagogy with great local cultural wealth.

1.5 Developing Effective Cybersecurity Frameworks for African Children

As the call for digital access through Africa continues to grow, it is imperative that we enhance the existing cybersecurity awareness for children (especially those in disadvantaged settings, such as refugee camps), as this expands. Such children come from a variety of backgrounds and experience very different challenges that require educational resources and tools that are culturally relevant, direct and age appropriate.

Culturally Relevant Pedagogy (CRP), created by Ladson-Billings [16], provides an avenue for this learning, by supporting the instruction design whilst balancing the needs of learners about the educational intent. When we make cultural connections/relationships with how we deliver digital safety education, we can make abstract ideas - like cybersecurity concepts - relatable. For example, finding a cultural or a story through use of African thematic comic books (aimed at engaging children), this is how the learner will make connections, and gain understanding and retention.

We propose a culturally grounded approach to delivering cybersecurity education for children, also illustrating how storytelling and illustrations can support children's future awareness and safety online.

Our work revolves around the research questions below:

1. **RQ1:** How does the use of professional illustrations and storytelling techniques in an African-themed cyber security comic book affect children's ability to comprehend cybersecurity concepts?
2. **RQ2:** How does an African-themed comic book effectively convey cybersecurity concepts to children with cultural relevance and engagement?
3. **RQ3:** How does an African-themed cybersecurity comic book measure up to other educational approaches aimed at expanding children's understanding and awareness of cyber threats and best practices?

2 Related Work: Cybersecurity Education for Children

Amidst a digital age that increasingly pervades all parts of our lives, children are plunging into the online oceans at younger ages. Much of this exploration starts on the Internet long before they turn nine, and from there, their world becomes a game, an endless space to play and learn. However, this early digital footprint can also pave the way for trouble. Cyberbullying, identity theft, and other shady internet behaviors are common, and perpetrators will take every opportunity to target unwary victims. Clearly, as children get older and become digitally literate, cybersecurity education will become more useful both within and outside of schools. Imagine a classroom full of eager students, all staring at an illustrated comic book that tells the story of a hero navigating a digital maze. That is what we offer as an innovative cybersecurity education method: multimedia storytelling to teach children about safety. When selecting lessons and culturally relevant stories for our online publications, we will prioritize stories of African cultural heritage. The combination of education and culture provides a highly powerful experience for children.

2.1 The Role of Culture in Learning

Culture relevance is central to the way children understand information. It can be incredibly important from the position of making sure that the messages are culturally relevant to children. An example study shows that when students can see a reflection of themselves and their experiences throughout the material, they are more likely to actively participate in learning. Phungula (2021) brings this understanding to African children's literature and the effect of cultural narratives on cognitive development [17]. They found that children appeared to learn more from stories or narratives containing aspects of culture that were aligned with their own cultural values- contributing to the children's cognitive development. They also noted that cultural narratives impart lessons and values that are important to children's cognitive and social development, but they also contribute to shaping identity.

Consider a young child reading about a clever rabbit that defeats a predator, similar to how the young child can outsmart a similar occurrence in their own life by being clever or intelligent. They can translate their learning into the narrative experiences of the story, making it a much more valuable reference for learning purposes.

Theron et al. (2017) offer a similar conceptualization in the form of resilience; In their writing, they demonstrate that culturally relevant stories teach children to be emotionally strong [18]. They found that stories can be a source of solace and something children can use as a guide in making decisions, essentially, in how to live their life.

However, despite these insights, many existing cybersecurity educational materials lack this cultural depth. They often use generic stories or characters that do not resonate with the children they aim to educate. This is where the proposed method shines. By weaving African cultural themes into the fabric of cybersecurity lessons, we can create a tapestry of knowledge that children not only learn from but also cherish.

2.2 The Power of Visual Storytelling

Comics and illustrations are not only fun for entertainment, but also impactful as educational materials. The visual format allows the interpreter to formulate complex ideas into easily understood concepts that are fun to read. Friedauer et al. (2022) created a comic for elementary school-aged children to awaken their interest in cybersecurity [19]. They created interesting colorful pictures and characters that kept the attention of young readers. They also created comics to teach high school students cybersecurity concepts, but each study demonstrates how visual messaging can serve important information to their target audience [20].

Not all studies support the use of comics for education. Barela et al. (2019) suggested that comics have the potential to engage children, but when comics are used with adult audiences, they often did not succeed [21]. The critique identifies an important aspect of instructional design: the content must align with the audience's needs and wants.

Our recommended method considers this by not only employing comics, but also emphasizing that the stories and illustrations are embedded in African cultural contexts. Imagine a child reading about a young hero, with new chapters based on old folklore, learning even how to fend off online villains. In this form of socially ascribed storytelling, an otherwise boring lesson becomes a journey.

2.3 Understanding the Audience

One of the most important aspects of providing education is targeting the right audience. Preteens are a less studied group because many studies mainly focus on particular age facets, such as Zhang-Lennedy et al. (2016) and Matthews et al. (2019) [22] [23]. It is critical to acknowledge this as preteens are the age group most at risk of online dangers and need a knowledge base to promote the development of their safety and digital thriving skills.

Our proposed method aims to develop awareness of cybersecurity among young people during a time of formative learning. Bridging this gap through the above

method not only teaches students, but also encourages students to be vigilant about their online safety. Just think of the dynamic inside the classroom, while the children are not simply an empty vessel to be filled with knowledge, they are engaged participants in their own learning - talking about what they think is relevant for online safety.

2.4 Connecting Culture and Cyber Safety: A Path Forward

In short, for children, the cyber world is both very positive and very dangerous. As children discover and navigate their virtual worlds, we need to prepare them with the tools and knowledge to protect themselves from attackers. The literature can provide substantial information on the issues surrounding cyber safety and security; however, the existing literature also reveals serious gaps, especially with regard to cultural relevance and audience engagement. The methodology we develop will address the gaps left by previous research by creating visually appealing learning materials for preteens that include African cultural narratives.

By creating links between knowledge and lived experiences, we not only have an opportunity to influence children as consumers of that knowledge, but we also have the chance to enable them to be agents in their own protection when it comes to their digital safety. In the future, we hope to be able to create an inclusive and culturally relevant cybersecurity education curriculum that will enable the next generation of users to interact constructively with cyberspace while also learning to mitigate the safety hazards that cyberspace can provide. As we move forward, we hope to envision a world in which every child is equipped with knowledge and resilience so that when they embark on their next digital journey, they are as confident and safe as the characters in their favorite stories.

2.5 Overview and Comparative Analysis of Related Work

The comparative summary of studies with cultural relevance is provided in Table 1. The table examines the methodological strengths and weaknesses of the quality of cultural relevance as embodied in educational materials. Most studies focus on the importance and need for cultural appropriateness, but do not pay substantial attention to the individual needs of distinct audiences. For example, Zhang-Lennedy et al. (2021) effectively used multimedia tools with students. However, they did not explore the potential of incorporating culturally rich narratives. In fact, including such narratives might support better understanding [24]. This indicates one of the larger problems of the many existing methods in the literature, many of which do not highlight the depth of cultural context needed to resonate with diverse audiences.

On the other hand, as described in Table 2, the use of audiovisual tools is vital in increasing the accuracy and appropriateness of instructional materials. We attempt to improve this insight by adding culturally appropriate imagery for African children, including those from underprivileged backgrounds like refugee camps. Typical treatments may ignore the use of images altogether or use stock images devoid of context; in contrast, our proposed framework focuses on providing effective visual educational

Table 1 Cultural Relevance in Selected Papers

Paper	Relevance Level	Findings	Notable Insight
Phungula (2021) [17]	High	Cultural elements crucial	Broader cultural narratives
Theron et al. (2017) [18]	High	Folktales boost resilience	Addresses diverse child challenges
Ladson-Billings (1995) [5]	High	Pedagogy rooted in relevance	Combines culture and media
Our Comics [25]	High	Culturally meaningful	Engaging for underrepresented learners
Friedauer et al. (2022) [19]	Medium	Security-focused	Encourages child content creation
Matthews et al. (2019) [22]	Medium	Cyber awareness improved	Interactive and relatable
Zhang-Lennedy et al. (2016) [23]	Medium	Design effectiveness	Integrates African themes
Buchanan et al. (2021) [26]	Medium	Diversity addressed	Practical application
Kemal (2022) [27]	Medium	Online safety in stories	Highlights cultural relevance
Ledbetter et al. (2016) [20]	Low	Simplified understanding	Youth-oriented focus
Barela et al. (2019) [21]	Low	Less effective for adults	Age-specific engagement

resources that encourage children's active participation, ownership, and meaningful connection to the learning process.

Table 2 Use of Visual Mediums in Selected Papers

Paper	Visual Medium	Key Findings	Design Strength
Friedauer et al. (2022) [19]	Comics	Positive security impact	Promotes child-generated content
Ledbetter et al. (2016) [20]	Comics	Enhances understanding	Focused on youth
Matthews et al. (2019) [22]	Story tool	Boosts awareness	Interactive and relatable
Zhang-Lennedy et al. (2021) [24]	Multimedia	Effective engagement	Integrates African culture
London (2020) [28]	Comics	Cybersecurity themes	Offers narrative variety
Kemal (2022) [27]	Comics	Online safety promotion	Emphasizes cultural fit
Our Comics [25]	Comics	Literacy improvement	Relevant and engaging content
Phungula (2021) [17]	None	Emphasizes culture	Uses storytelling
Jeong et al. (2020) [29]	None	Symbol-based interpretation	Age-appropriate focus

While existing studies in cybersecurity education for children have made valuable contributions, many fall short in areas critical to long-term engagement and contextual relevance. As summarized in Table 3, several prior works rely on generic visual tools, minimal cultural adaptation, or limited child involvement. Our proposed framework addresses these gaps by centering African children's lived experiences, employing co-created visual storytelling, and aligning instructional content with both cultural and pedagogical best practices. This comparison highlights not only the novelty of our approach but also its potential for broader applicability in underserved contexts.

Table 3 Comparison Between Prior Studies and Our Proposed Framework

Aspect	**Prior Studies**	**Our Proposed Framework**
Cultural Relevance	Often assumed or generalized (e.g., Ledbetter et al., 2016; Choong et al., 2019)	Specifically designed for African children, including those in refugee communities
Visual Engagement	Used generically or not at all; visuals not tailored (e.g., Zhang-Lennedy et al., 2016)	Uses culturally adapted comics co-created with children
Child Participation	Children treated as passive recipients (e.g., Barela et al., 2019)	Children involved as co-creators in both design and testing
Pedagogical Approach	Focus on awareness or security concepts without personalization (e.g., Siddiqui & Zeeshan, 2020)	Integrates narrative-based, learner-centered pedagogy
Practical Impact	Limited validation or real-world deployment (e.g., Buchanan et al., 2021)	Field-tested in diverse educational settings for contextual effectiveness

3 Methods

In this section, we provide thorough elaboration on the proposed methods intended for executing the experiment. This contains a thorough explanation of both our proposed fictional and human characters, with the heroes being cyber defenders and helpers and the villains being cyber attackers and malware as well as the scope of work.

3.1 Area of Focus

There are a variety of cybersecurity attacks affecting individuals online. As children are also identified as part of the users of the Internet, they are not ignored by attackers. Common themes have been identified in relation to the cyberattacks that children face while using the Internet. These attacks are grouped in the following themes: pop-up/Malware, cyberbullying, cyberstalking, and social engineering. Their definition and importance in relation to the subject matter follow in the following sections. An assessment of how these threats affect children have also been made.

3.1.1 Malware and Viruses

Malicious programs can result in unauthorized access to personal information, including sensitive data like login credentials and banking details. They can also compromise device security, leading to data loss, system crashes, and even remote control by attackers. Preteens are especially vulnerable to these threats due to their limited understanding of online risks and their tendency to engage in risky online behaviors. Malware and viruses targeting preteens online is a concerning issue in today's digital landscape. Attackers employ various tactics to exploit vulnerabilities and target unsuspecting children. As emphasized by the DQ Institute in their 2023 report, approximately 70% of children aged 8 to 12 years have faced cyber risks, including malware and viruses, while using the Internet [1]. A study published by Norton in 2019 revealed that 1 in 4 children have accidentally downloaded malware while browsing the Internet [30]. Malware and viruses pose significant risks to individuals, particularly to preteens, who use the Internet.

3.1.2 Cyberbullying

The Cambridge dictionary defines cyberbullying as "the activity of using the Internet to harm or frighten another person, especially by sending them unpleasant messages" [31]. UNICEF defines cyberbullying simply as "bullying with the use of digital technologies" [32]. This could occur on social media platforms as well as messaging platforms, gaming platforms, and on mobile phones. Cyberbullying depicts repeated behavior that is meant to scare, anger or shame victims. These behaviors span from spreading lies to sending hurtful, abusive, and threatening messages. Effects of cyberbullying are long-lasting. Cyberbullying affects individuals mentally (by making them upset, afraid or angry), emotionally (by making them feel ashamed) and physically (through tiredness caused by a lack of sleep).

Cyberbullying has been identified as one of the common cyber threats targeted at teenagers and kids. With an emphasis on the effects of cyberbullying on the mental health of children, it has been shown that children subject to cyberbullying feel ashamed, nervous as well as insecure about the perceptions others have of them. This results in children isolating themselves and even skipping school [33]. According to Security.org, 21% of children aged between 10 and 18 globally have been victims of cyberbullying. 56% of the reports on the occurrence of such were made between January and July 2020 with the advent of COVID-19 lock downs. In addition, the research showed that children on YouTube are most likely to be cyberbullied at a likelihood of 79%, followed by SnapChat, Tiktok and Facebook at respective chances of 69, 64 and 49% [34].

3.1.3 Cyberstalking

Compiling internet data in relation to harassing or stalking someone else is known as cyberstalking. Cyberstalkers employ electronic media, such as online services or the Internet, to track down their victims. Cyberstalkers may get fixated on the victim, either out of an obsession with their love and respect or out of jealousy (particularly if

the victim has dumped them). They may also use hate speech to vent their frustrations before leaving the victim, feeling deceived and betrayed.

Roughly 7.5 million persons, including children, are victims of stalking in the United States each year [35]. Although the impact on victims should not be understated, this statistic highlights how common stalking is. The prevalence of cyberstalking victims varies around the world (for example, 62% in Portugal and 11.9% in China) [33]. This has emphasised the severe effects and prevalence of cyberstalking in various regions of the world.

Cyberstalkers may engage in various behaviors, including closely monitoring or following specific individuals they are fixated on. Some may track the online activities of their targets, potentially following a wide range of accounts to gather information or observe patterns. The impact of such behavior can vary, but it often contributes to the following:

1. Psychological Impact: In certain situations, victims endure agitation, anxiety, and, in the worst instance, suicidal thoughts. An assault of persistent harassment and invasive behaviour can lead to chronic stress and a sense of helplessness, which can worsen the mental health of the victimised party.

2. Impact on Individual Health: The psychological strain caused by cyberstalking may give rise to additional physical issues. Headaches and other serious problems with sleep are examples of these stress-related health issues. The immune system's capacity to fight off infections can be weakened by ongoing stress, too.

3. Impact on Social Life: Cyberstalking can be detrimental to an individual's social life, leading to self-doubt and the development of nearly unrealistic expectations among others. A person's isolation and difficulties forming relationships with others may result from their withdrawal from social and cultural links. One problem that this population faces is the possibility of stalking, which can hinder their social interactions and lower their general quality of life.

3.1.4 Social Engineering

Social engineering refers to a sophisticated set of tactics aimed at manipulating individuals into divulging confidential information or engaging in activities that are detrimental to their security and privacy. Phishing, a prominent form of social engineering, involves various techniques such as pretexting, baiting, quid pro quo, and tailgating. These tactics capitalise on human psychology, exploiting trust and curiosity to achieve malicious goals. Phishing attacks often utilise psychological manipulation to lure unsuspecting victims into revealing sensitive information, clicking on malicious links, or downloading malicious attachments.

Recent global trends indicate an alarming rise in cyberattacks targeting children, particularly through social engineering tactics. A concerning report from Kaspersky revealed that cybercriminals orchestrated over 7 million attacks on popular children's gaming titles in 2022 alone [36]. These attacks encompass applications that imitate widely recognized games like Roblox, Minecraft, and Fortnite, specifically designed to target devices used by parents. This approach capitalises on the trust that parents may place in these seemingly harmless children's games, ultimately compromising their devices and potentially exposing sensitive information.

3.2 The Study Design

In this study, we adopted an experimental design, focusing on five schools in Rwanda. These schools included two private schools (an international private school and a local private school) and three public schools (one urban public school, one rural public school, and one school situated in a refugee camp in rural settings). We had a total of 300 students, with students randomly assigned to either an experimental group or a control group, with 150 students in each. The experimental group read the comic book, while the control group simply received written notes on the same story.

The term 'experimental group' refers to a subgroup of research subjects that would be used for the main experiment, i.e., the subgroup that would be used to test the main hypothesis, which is, in this case, that the comic would outperform traditional notes in educating children about online safety. This group would be given comic books to read.

A random sampling strategy was adopted to select the students participating in this study. Randomly generated IDs of the students of grade 6 (upper primary) were obtained directly from the school, and a selection of names for the sample was done randomly. Particular attention was paid to having a fair representation for the study. To that effect, a balanced representation of males and females was made, where both genders were equally considered.

In this study, it was imperative to gauge the students' understanding of the subject matter. Assessing their knowledge beforehand allowed us to determine their familiarity with online safety concepts. The pre-assessment was crucial for evaluating the efficacy of the instructional materials used to teach them about online safety and objectively comparing the relevance of comic books versus written notes in education. To accomplish this, all participants took a pre-assessment comprising ten questions covering topics such as cyberbullying, cyberstalking, pop-up/malware, and social engineering, with their scores being recorded accordingly.

Following the experiment, particularly after engaging with the materials, participants took a post-assessment. We devised sets of questions for both the pre-assessment and post-assessment to be utilized in the experiment. A comparison was made between their scores on both assessments to evaluate the effectiveness of the comic books relative to the traditional notes. Further comparative analysis was conducted for private, public, and refugee camp schools.

4 Recruitment of the Participants

The process through which minors were recruited is outlined below, including obtaining their assents and securing full approvals and consents from their parents or guardians.

4.1 Target Population and Participant Eligibility

Participants consisted of 300 minors aged 9 to 13 years, enrolled in purposively sampled schools in Rwanda. Schools included both rural and urban settings to ensure

representation across different contexts. Eligible participants demonstrated the ability to read English or Kinyarwanda at their respective grade levels.

4.2 Process for Obtaining Consent and Assent

Parental consent forms were distributed through school staff, outlining the study's objectives, procedures, and the rights of participants. Parents provided signed consent for their child's participation. Following parental consent, children were approached by the research team for assent using age-appropriate language. The assent process emphasized the child's right to withdraw at any time, regardless of parental consent. Written assent was obtained before enrollment.

4.3 Study Activities and Timeline

The study involved four activities: (1) a pre-assessment quiz on cybersecurity knowledge, (2) exposure to the comic book intervention or a standard text, (3) a post-assessment quiz, and (4) a Likert scale questionnaire assessing satisfaction with the materials. These activities were conducted over five days within school hours. Each session was designed to minimize disruptions to the academic schedule.

4.4 Ethical Approvals

The study was approved by Carnegie Mellon University's Institutional Review Board (IRB) and the Government of Rwanda through the National Ethics Committee (RNEC). Ethical oversight ensured adherence to guidelines protecting the rights and well-being of participants.

4.5 Measures for Data Security and Confidentiality

Participants' data were anonymized using coded identifiers, such as MMIS4-G6, which stands for Mother Mary International School number 4, Grade 6. Data were securely stored in a password-protected institutional Google Drive, accessible only to authorized research personnel. Identifiable information was not collected.

4.6 Addressing Potential Risks

Potential emotional triggers related to discussions on online risks were addressed by training the research team to recognize and respond to signs of distress. A pediatric psychologist was available to provide counseling services if required.

5 Development and Ideation of the Comic Book

When we hear the word comics, we immediately see magnificent images of Batman and Captain America; Spider-Man even comes to mind. However, comic books have been generally overlooked as a cultural currency, despite being an equally wide and possibly even more vital frontier. In the context of African communities, we developed an African-themed comic book that introduces original characters—cyberheroes—who

embody local cultural values and address specific cybersecurity challenges faced by preteens and marginalized groups.

5.1 Human Characters

Meet Maya, Juma, Zuri, and Imani, four children from a vibrant African community, each grappling with their own encounters with cyber-attacks that leave them feeling unhappy and discouraged. To empower them in their struggles, we designed a team of original characters known as African Cyberheroes—GuardianShield, CyberShield, and Firewall—led by the charismatic Captain Cyber, steps in to save the day. By drawing inspiration from the unique storytelling traditions found in African comics, manga, and webtoons, this project seeks to create engaging narratives that not only educate but also empower young readers.

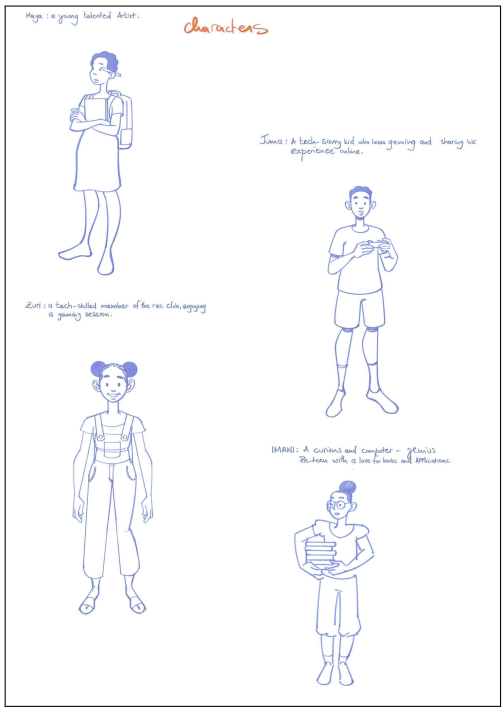


Fig. 1 Digital pen sketches of Maya, Juma, Zuri and Imani representing human characters (cyber-attack victims).

The design process for these human characters involved initial pencil sketches, similar to the Cyber Heroes, which were then refined digitally to enhance their details and clarity. This process is depicted in Figure 1. Integrating elements from distinctive African art styles enhances relatability and effectiveness in conveying crucial cybersecurity concepts. Ultimately, this initiative aims to foster a stronger understanding of

online safety within culturally familiar frameworks, allowing children to see themselves as active participants in their digital safety.

5.2 The Cyber Heroes

In contrast to the human characters, the Cyber Heroes are designed to play a more active role in addressing cyber threats. The Cyber Heroes include characters such as Guardian Shield, Cyber Shield, and Firewall, led by the charismatic Captain Cyber. These characters are envisioned to embody various aspects of cybersecurity and serve as role models for young readers.

The design process for the Cyber Heroes involved sketching initial designs with pencils, which were then refined and detailed using a tablet pen. This approach is similar to the process used for the human characters, as illustrated in Figure 2. The digital refinement process allows for adjustments and enhancements to ensure that the characters effectively convey the intended cybersecurity messages and engage the audience.

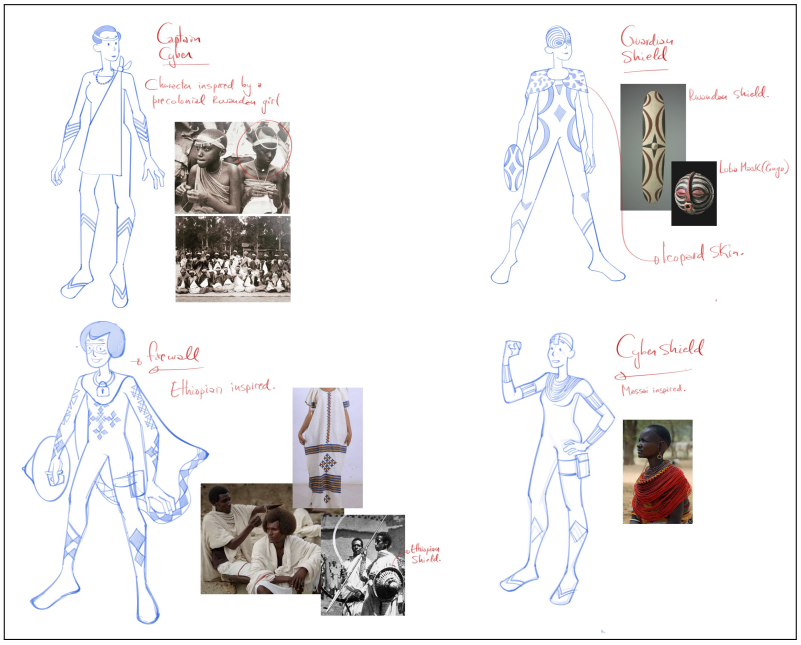


Fig. 2 Digital pen sketches of the Cyber Heroes

5.2.1 Captain Cyber

The main protagonist who leads the operations of the cyber heroes to help the children recognize and counter cyber threats. This character is inspired by a precolonial Rwandan girl, featuring an Amasunzu haircut, a Tiara Headband, and a shoulder drape as shown in Figure 3. The intricate triangular patterns on her tight costume

draw inspiration from the renowned ancient Rwandan artistry known as Imigongo. Inspired by Rwanda's cultural heritage, particularly the iconic "Amasunzu" hairstyle, the character embodies traits of bravery, power, and nobility. Historically, this hairstyle symbolized strength and influence within Rwandan society, commanding respect and admiration. By evoking this imagery, the character is envisioned to have a profound impact in cyber defense. The association with the Amasunzu hairstyle signifies the character's resilience and leadership qualities. Like the pre-colonial Rwandan woman, she is a formidable force, inspiring others in the fight against cyber threats. Her bravery and nobility serve as a testament to her potential to lead and overcome challenges posed by cyber adversaries.



Fig. 3 The Captain: Leading the Cyberheroes inspired by a pre-Colonial Rwandan woman with the 'Amasunzu' hairstyle. The woman photo is by Lee Tracy, used under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 United States License [37].

5.2.2 Guard Shield

This cyber hero plays a pivotal role in addressing cyber stalking incidents targeting a child online. When faced with cyber stalking, Guard Shield steps in to assist the targeted child. His role is to educate the compromised child on the significance of maintaining online privacy and the potential dangers associated with sharing personal information on social media platforms. Among other roles, Guard Shield insists the importance of exercising caution when interacting with strangers online and emphasizes the need to recognize warning signs of cyber stalking, empowering the child to navigate online spaces safely.

Inspired by the cultural heritage of Africa, Guard Shield draws upon the symbolism of the Luba Kifwebe mask from the Congo and the Ingabo Rwandan shield, as depicted in Figure 4. The Luba Kifwebe mask holds profound cultural and artistic significance within Luba society, often associated with secretive societies that safeguarded the heritage of the Luba Empire and fostered social cohesion among its diverse population. Similarly, the Ingabo Rwandan shield, crafted from wood and adorned

with natural pigments and ancient markings, served both ceremonial and combat purposes. Its complex designs, imbued with symbolic motifs, were intended to instill fear in adversaries while providing protection to its wielder. By embodying these cultural elements, GuardShield symbolizes resilience, protection, and vigilance in combating cyber threats and safeguarding the digital well-being of children.



Fig. 4 GuardShield inspirations: Congolese Luba Kifwebe mask and Ingabo Rwandan shield [38].

5.2.3 Cyber Shield

She is a key member of the Cyber Heroes team and one of her roles is to assist a child facing a phishing attack. She emphasizes being cautious with personal information on the Internet. She teaches how to distinguish between legitimate and fraudulent emails and links, which aim to trick children into revealing their personal information.

Cyber Shield provides vital guidance on spotting phishing attacks, offering simple yet effective strategies. She additionally emphasizes the need to verify requests through official channels, advocating direct communication with trusted sources to confirm message authenticity. This proactive approach empowers children to confidently authenticate communications, reducing the risk of falling prey to phishing schemes. In essence, Cyber Shield equips children with concise techniques to navigate the digital realm securely, fostering a culture of skepticism and proactive verification to safeguard personal information and assets.

As illustrated in Figure 5, this character draws its inspiration from the Maasai women of Kenya and Tanzania, where colors carry deep symbolic meanings. In Kenya's and Tanzania's diverse culture, the vibrant reds in clothing and detailed beadwork symbolize qualities like courage, bravery, and strength. We specifically chose this character to represent CyberShield's toughness and potential to make a big impact in defending against cyber threats. With the rich symbolism of the Maasai woman's attire, CyberShield stands as a strong protector in the digital world, ready to face any challenges head-on.



Fig. 5 CyberShield character: Empowering defense against cyber threats, inspired by Maasai Woman. Image © Monika Ettlin, licensed under Creative Commons Attribution-NonCommercial-ShareAlike 2.0 [39].

5.2.4 Firewall

As an integral member of the Cyber Heroes team, Firewall plays a crucial role in aiding a child in thwarting an imminent malware attack. With precision and clarity, Firewall delves into the complexities of malware and viruses, explaining their malicious operations to the young individual. Going beyond mere explanation, Firewall passionately emphasizes the critical importance of device security, cautioning against the risks associated with downloading unfamiliar files.

Furthermore, Firewall ardently promotes various preventive measures against malware and viruses. This includes advocating for regular security software updates, performing proactive malware scans, and fostering safe browsing practices. Through his vigilant guidance, Firewall emerges as a steadfast protector, equipping both children and peers with the necessary tools and knowledge to navigate the digital landscape securely.

Taking inspiration from Ethiopian shields known as “Tafa” or “Gasha” referenced in Figure 6, Firewall’s character embodies the emblem of protection deeply rooted in Amhara culture. Symbolizing bravery and defense, these shields were traditionally carried by youths alongside esteemed leaders, highlighting their significance and assurance. Thus, when readers witness Firewall wielding the Tafa, an inherent sense of protection is evoked, resonating with the character’s resolute commitment to shielding against digital threats.

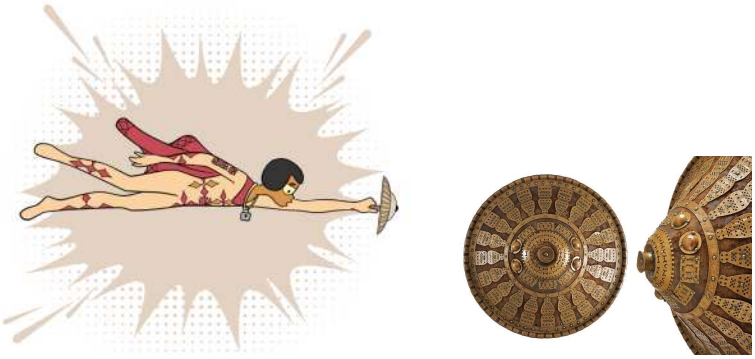


Fig. 6 The Firewall: Safeguarding against malware, inspired by the Ethiopian Tafa Gasha shield. Original shield image © Czerny's International Auction House, retrieved from [40].

We have summarized the Cyber Heroes characters in a single ink illustration, accompanied by a synopsis detailing the inspiration behind each character as shown in Figure 7. This comprehensive overview captures the essence and background of each hero, providing a clear understanding of their unique traits and the cultural or educational elements that inspired their creation.

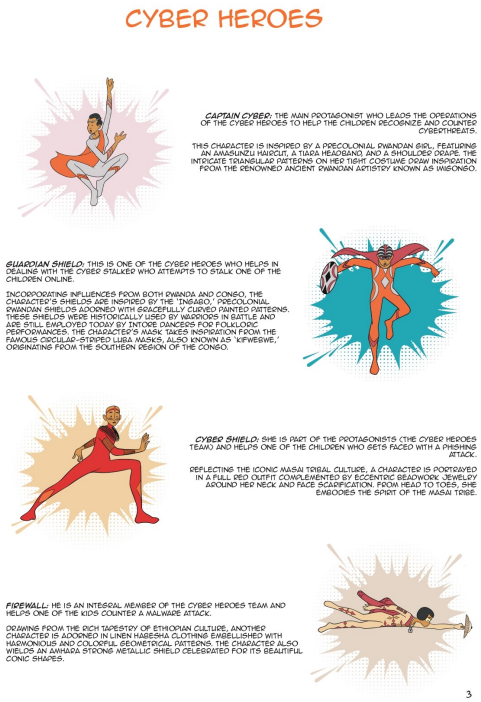


Fig. 7 Cyber Heroes inspiration summary.

5.3 The Cyber Villains

In this paper, the villains/attackers are the bad guys who exploit threats to carry out attacks. They include Phantom, Cyberstalker, Malware, Cyberbully, and Phisher, each representing a different role in attacking preteens online. Their actions emphasize how crucial online safety is and also serve as a case study for understanding various attacks and security precautions to avoid and recover from attacks.

5.3.1 The Cyberbully

This is the robotized villain that launches cyberbully attacks on children when they are online. Preteens are targeted by Cyberbully for a variety of reasons, including amusement, seeking revenge, or inflicting emotional harm on the victims. In the story, the heroes advised to always report Cyberbully and save screenshots of his messages as evidence.

5.3.2 The Cyberstalker

This is the villain who stalks one of the kids on social media. He contacted the kid through a popular gaming platform. Cyberstalker send repeated messages to harass, control, and intimidate preteens online. In the book the heroes advise to always block and report Cyberstalker and also seek help in case a Cyberstalker attacks you.

5.3.3 The Malware

In the story, the cyber heroes warn the kids to be cautious and watchful for their safety. This virtual villain is the mastermind behind the wave of malware attacks that infect children's devices through infected files. The malware is secretly spread by tricking users into clicking on malicious links that appear to be exciting news. Once the malware is released, it slows down the device and prevents the owner from accessing certain files. Within the narrative, the cyber heroes caution individuals to exercise caution and vigilance to ensure their safety..

5.3.4 The Phisher

A villain responsible for launching social engineering attacks mainly through phishing attacks. Phisher sends deceptive urgent action emails requesting credential login pretending to be verification requests. Phisher's emails appear to be trusted. For this reason, it is crucial to be cautious with personal information online, and staying alert is essential to avoiding falling victim to phishing scams. Figure 8 below summarizes the digital pen sketch of the Cyber Villains.



Fig. 8 Digital pen sketches of the Cyber Villains.

6 The Storyline

The storyline serves as a blueprint to aid easy illustration in crafting the comic book. The stories are divided into scenes, each portraying distinct cyber-attack scenarios, including cyberbullying, cyberstalking, phishing, malware, and viruses, and demonstrating their resolutions. This structured approach not only simplifies learning but also immerses the narrative in an engaging African context. By presenting relatable scenarios and culturally relevant elements, the storyline effectively promotes online safety among African preteens. The heroes' interventions in each scene provide practical tips and strategies, making the educational content both entertaining and impactful. We present the storyline below in form of four chapters.

6.1 Chapter 1: Cyberbullying

Maya, a friendly and talented student at the primary school in the quiet town of Gisenyi, has always been active on social media. She loves sharing her drawings and connecting with friends online. However, things take a turn for the worse when she starts receiving hurtful messages and comments from a stranger. These stranger stands to be a programmed villain called the "Cyberbully". Due to this, Maya becomes increasingly sad and confused, wondering why someone would say such mean things about her.

One day, as Maya is upset about the messages, she breaks into tears at school thinking she is alone but Captain Cyber hears her cries. Captain Cyber expresses concern about Maya's well-being and asks if everything is alright. Captain Cyber consoles Maya and asks her what is wrong. Maya decides to confide in Captain Cyber

about the cyberbullying she's been experiencing. Captain Cyber felt sorry for Maya assuring her that she is not alone and that they are there to help. The cyber hero explains that what Maya is going through is called cyberbullying and that it is a form of online harassment. Captain Cyber guides Maya on strategies to deal with cyberbullying effectively. She explains the importance of not responding to the cyberbully, as it encourages them to continue their action. Instead, she encouraged Maya to block the bully, which would prevent them from further contacting her. Additionally, Captain Cyber advises Maya to take pictures and save them as evidence of the cyberbullying incidents, as they may be useful when reporting the bully.

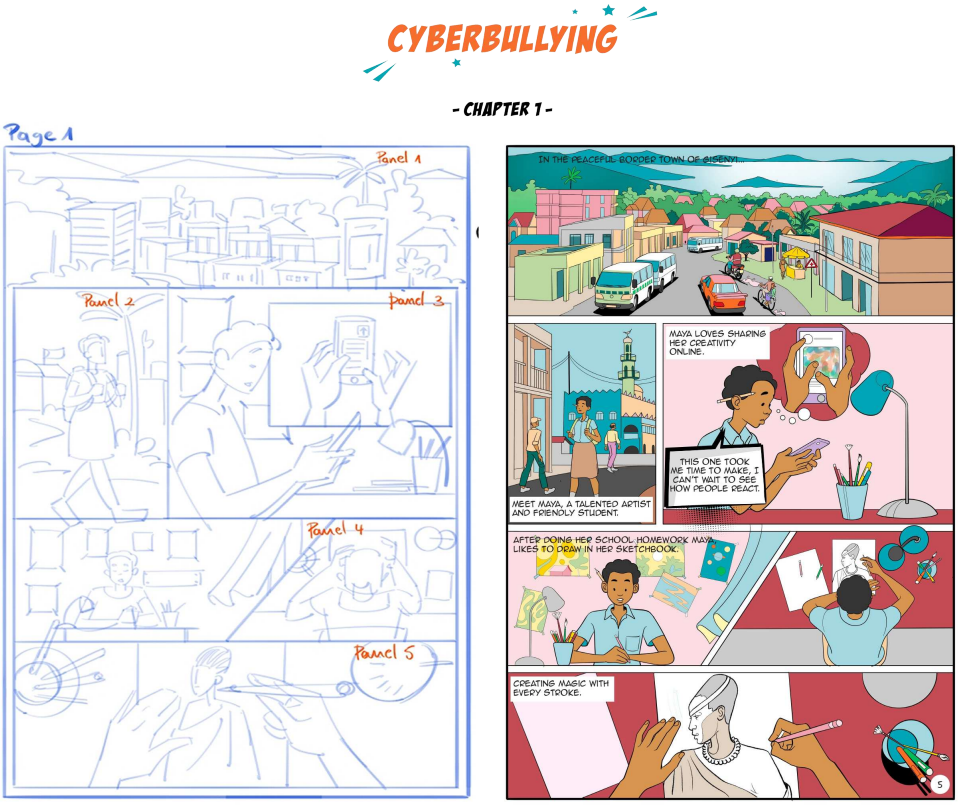


Fig. 9 Chapter 1 of 4, Page 1 of 5 - Conversion from digital pen storyboard to inked illustration. The rest of the Chapter is available in reference [41].

Captain Cyber highlights the importance of reporting the issue to a trusted adult, such as a parent, teacher, or school counselor. She assured Maya that reaching out for help is not a sign of weakness but rather a smart step towards resolving the issue. Captain Cyber also added that adults can give important guidance and support during such challenging times. Captain Cyber and Maya worked together to draft a message

to Maya's parents, explaining the cyberbullying incidents and seeking their assistance. They also discussed the importance of surrounding oneself with positive influences and supportive friends both online and offline. Through this scenario, preteens learn about the harmful effects of cyberbullying and the importance of seeking help when faced with such situations. The interaction with Captain Cyber guides how to handle cyberbullying effectively, including blocking the bully, saving evidence, and confiding in trusted adults. The narrative promotes empathy, resilience, and the understanding that no one should tolerate cyberbullying alone. For additional information on this chapter, please refer to Figure 9, which contains a link to access the rest of the chapter.

6.2 Chapter 2: Cyberstalking

Juma is a kid, comfortable with the use of technology, who loves gaming and frequently shares his gaming experiences and personal details on social media. One day, while exploring a gaming forum as expressed in Figure 10, he encounters a user who shares his passion for gaming. Excited to connect with someone who has the same interests. Juma engages in conversation with this new online friend. At first, the conversations between Juma and the stranger were casual and centered around their shared gaming interests. However, over time, the stranger's messages become increasingly strange and intimidating. The stranger started stating personal information about Juma's life that was never shared publicly. Juma begins to feel uneasy and alarmed by the situation. The stranger was no person other than the infamous Cyberstalker who had the reputation of stalking kids who patronize gaming platforms.

The cyber heroes, who have been checking online activities, notice the disturbing interactions between Juma and Cyberstalker. They quickly intervene to protect Juma and provide guidance in dealing with the cyber stalker. One of the cyber heroes, named Guardian Shield, approaches Juma calmly. Guardian Shield acknowledges Juma's discomfort and explains the concept of cyber stalking. The hero assured Juma that he is not alone and that the cyber heroes are there to help him.

Guardian Shield guides Juma through a conversation about the importance of online privacy and the potential risks of sharing personal information on social media. He stresses the need to be careful about interacting with strangers online and the importance of recognizing warning signs of cyberstalking. To empower Juma with knowledge and strategies to handle the situation, Guardian Shield provides him with the following guidance:

i. **Block and report:** Guardian Shield advises Juma to immediately block Cyberstalker and report the incident to the administrators of the gaming forum. They explain how blocking and reporting can help prevent further contact with the cyber stalker.
ii. **Preserve evidence:** Guardian Shield encourages Juma to take screenshots or keep records of the messages sent by Cyberstalker. This evidence can be crucial in reporting the incident to the appropriate authorities and ensuring his safety.
iii. **Seek adult help:** Guardian Shield urges Juma to inform a trusted adult, such as a parent, teacher, or guardian, about the situation. He emphasized the importance

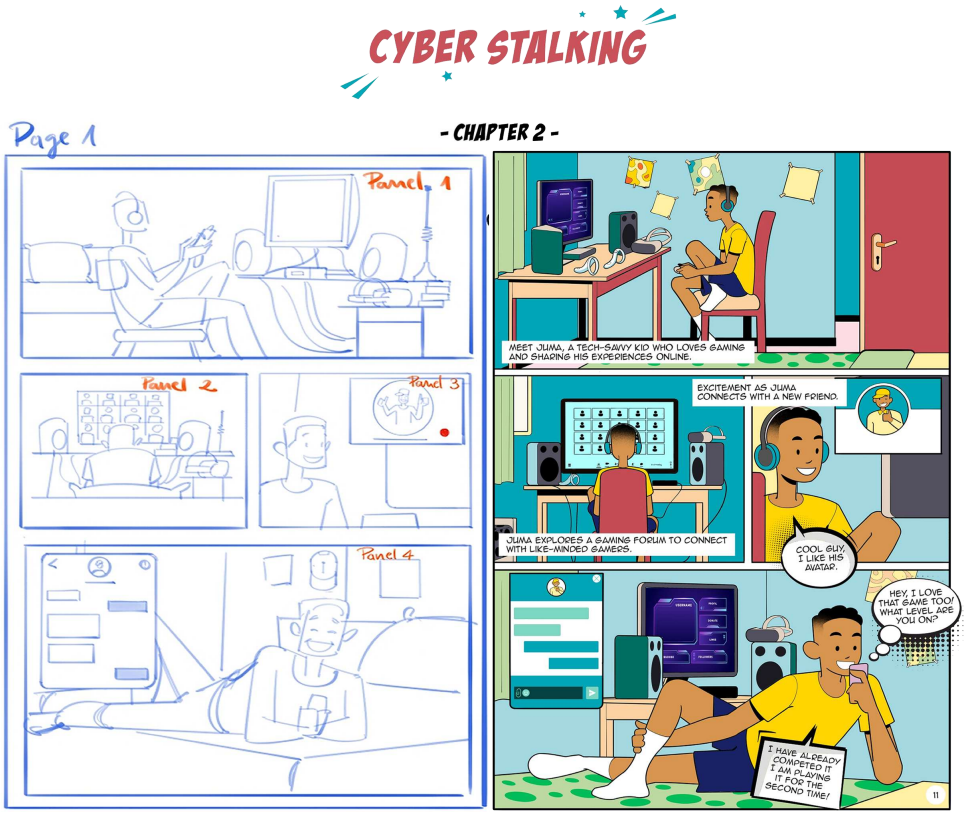


Fig. 10 Chapter 2 of 4, page 1 of 6 - transition from digital pen storyboard to inked illustration. Available here [42].

of seeking support and guidance from responsible adults who can help handle the cyber stalking incident effectively.

Guardian Shield reassures Juma that by taking these steps, he is actively protecting himself and regaining control over the situation. He emphasized that cyber stalking is a serious matter and should never be ignored or taken lightly.

Through this scenario, preteens learn about the potential risks of sharing personal information online and the alarming consequences of cyber stalking. The interaction with Guardian Shield highlights the importance of online privacy, recognizing warning signs, and taking immediate action to protect oneself. The narrative aims to raise awareness about cyber stalking and empower preteens to stay vigilant, seek help from trusted adults, and prioritize their online safety.

6.3 Chapter 3: Phishing

Zuri, a passionate gamer and tech-skilled member of the Rec Club, regularly receives emails related to gaming updates, promotions, and news. One day, she notices an email that appears to come from a popular gaming website she frequently visits. The email claims that her account needs to be updated to access new features and requests her login credentials for verification purposes. Despite the professional appearance and the presence of the gaming website's logo, Zuri senses something suspicious about the email. She recalls the lessons taught by the cyber heroes about being cautious with personal information.

One of the cyber heroes, CyberShield, notices Zuri's concern and decides to assist her in navigating this potential phishing attempt. CyberShield approaches Zuri and praises her for trusting her instincts. CyberShield explains that the email she received is an example of a phishing attempt, where cybercriminals impersonate trusted organizations to trick individuals into revealing personal information, such as usernames, passwords, or credit card details.

CyberShield elaborates on phishing, describing it as a form of social engineering attack. These attacks lead users to make security mistakes or disclose sensitive information. Phishing emails often use deceptive tactics to create a sense of urgency or lure victims into immediate action. They also employ impersonation, where attackers pretend to be someone they are not to commit fraudulent transactions. More details about this chapter are available in the provided link in the caption of Figure 11 below.

To empower Zuri with knowledge and skills to identify phishing attempts, CyberShield provides her with the following guidance:

i. **Examine Email Addresses and Links:** CyberShield encourages Zuri to carefully inspect the sender's email address. She explains that phishing emails often originate from addresses designed to mimic legitimate ones but may contain slight variations or unfamiliar domain names. Zuri is also advised to avoid clicking on any suspicious links within the email, as they may redirect her to malicious websites designed to steal her credentials.
ii. **Verify the Source:** CyberShield advises Zuri to independently verify the email's legitimacy by visiting the official website of the gaming platform directly. She demonstrates how to navigate to the website using a trusted browser and emphasizes avoiding any links provided in the email, as they could lead to fraudulent sites.
iii. **Be Cautious of Urgent Requests:** CyberShield highlights that phishing emails often employ tactics to create a false sense of urgency, prompting hasty actions. She advises Zuri to remain calm, take her time, and critically assess the content of the email before responding or providing any personal or sensitive information.
iv. **Report the Phishing Attempt:** CyberShield encourages Zuri to report the suspicious email to the official support team of the gaming platform. She explains that reporting such phishing attempts not only protects Zuri but also helps the organization safeguard other users from falling victim to the same scam.

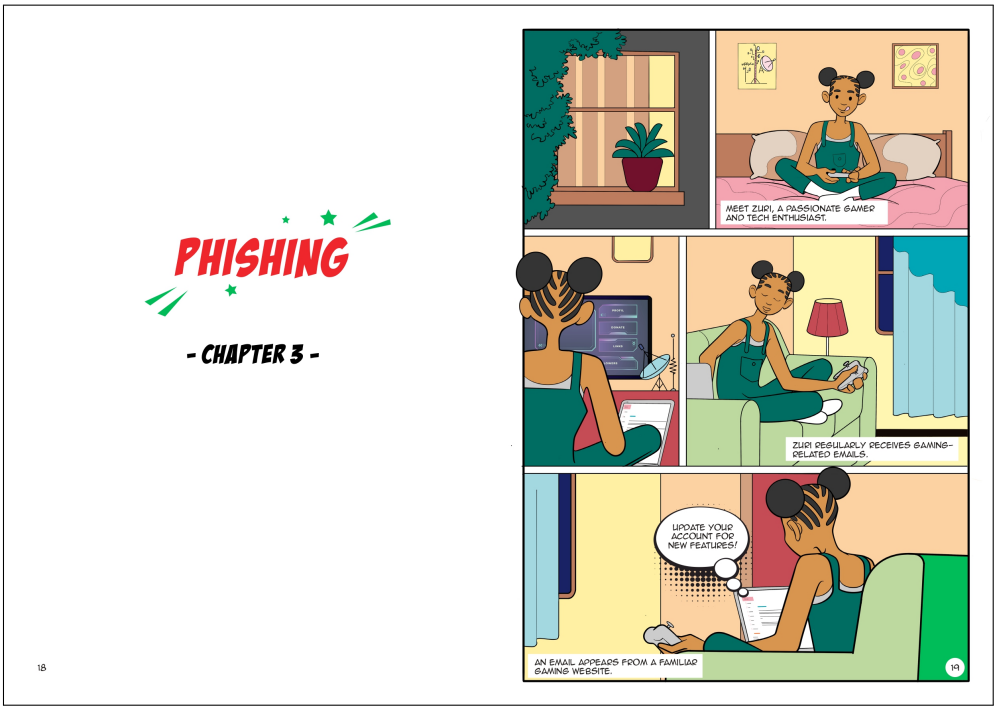


Fig. 11 Chapter 3 of 4, page 1 of 7 as seen in [43].

CyberShield reassures Zuri that she did the right thing by trusting her instincts and seeking help. She commends Zuri for her vigilance and emphasizes the importance of staying cautious in the online world. Through this scenario, preteens learn about the deceptive tactics used in phishing attempts and the potential risks of revealing personal information to unknown sources. The interaction with CyberShield provides practical guidance on identifying phishing emails, verifying the legitimacy of requests, and taking appropriate actions to protect oneself from falling victim to phishing attacks. The narrative promotes critical thinking, online safety awareness, and the understanding that phishing is a prevalent threat that requires caution and vigilance.

6.4 Chapter 4: Malware and Viruses

In the final chapter, depicted in Figure 12, Imani, a creative student with a passion for coding and exploring new software, inadvertently downloads a malicious file that masquerades as a free software update. Shortly thereafter, her computer starts exhibiting unusual behavior: it displays pop-up ads, experiences a significant slowdown, and begins to malfunction. It becomes clear to Imani that her computer has been infected by malware.

The cyber heroes, who are always alert to online threats, notice Imani's distress and decide to intervene. One of the cyber heroes, named Firewall, approaches Imani with a friendly and supportive attitude. Firewall explains that her computer has been

infected by malware, which is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.

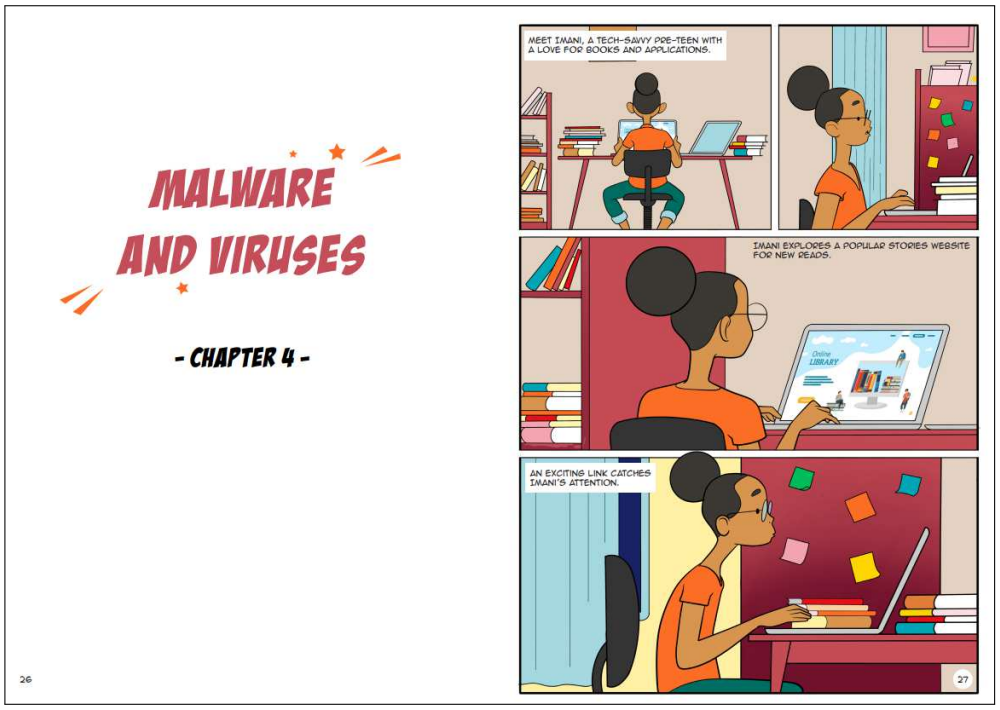


Fig. 12 Chapter 4 of 4, page 1 of 7 as referred in [44].

Firewall offers the following guidance to help Imani deal with the malware infection and protect her computer in the future:

i. **Disconnect from the Internet:** Firewall advises Imani to immediately disconnect her computer from the Internet to prevent the malware from communicating with its source and causing further damage.
ii. **Run a full antivirus scan:** Firewall explains the importance of having reliable antivirus software installed on her computer. He guides Imani through running a full system scan to identify and remove the malware. He also advises her to keep the antivirus software up to date to ensure maximum protection against new threats.
iii. **Avoid downloading from untrusted sources:** Firewall emphasizes the importance of downloading software and updates only from reputable sources. He explains that downloading files from unknown or unverified websites can expose her computer to malware and other security risks.

iv. **Enable automatic updates:** Firewall advises Imani to enable automatic updates for her operating system and software. These updates often include security patches that can protect her computer from known vulnerabilities exploited by malware.

Firewall reassures Imani that by following these steps, she can regain control of her computer and prevent future malware infections. He commends her for her proactive approach to seeking help and emphasizes the importance of staying informed about online threats. Through this scenario, preteens learn about the risks of downloading files from untrusted sources and the potential consequences of malware infections. The interaction with Firewall provides practical guidance on dealing with malware, running antivirus scans, and adopting safe online practices. The narrative promotes cybersecurity awareness, responsible online behavior, and the understanding that proactive measures can protect against malware and other online threats.

7 Results Analysis and Discussion

This section presents the findings from the study, highlighting the effectiveness of the comic book intervention in improving cybersecurity knowledge among students from diverse socioeconomic backgrounds. The analysis integrates statistical evaluations of pre- and post-test scores with detailed insights from student feedback, providing a comprehensive assessment of the intervention's impact and engagement levels.

7.1 Statistical Analysis of Pre- and Post-Test Scores

A paired sample t-test was used to evaluate the hypothesis that the intervention significantly enhanced students' cybersecurity knowledge. The significant improvements across all schools provide strong evidence that the comic book intervention effectively increased students' understanding of cybersecurity concepts.

The paired t-test statistic is calculated as:

$$t = \frac{\overline{d}}{s_d/\sqrt{n}}, \tag{1}$$

where:

- $\overline{d}$ is the mean difference between pre-test and post-test scores,
- s_d is the standard deviation of the differences,
- n is the number of participants.

Statistical analysis demonstrates that the comic book intervention was effective in various learning environments as elaborated in Table 4. In well-resourced schools like Mother Mary International School and Kigali Parents School, the intervention built upon existing educational structures to enhance learning. In contrast, G.S. Paysannat, located in a refugee camp, and rural schools like Rugeshi Primary School showed the most substantial gains, underlining the comic's adaptability and its potential to

Table 4 Stats Summary: Pre vs Post Scores

School	Pre	Post	SD_1	SD_2	t-stat	p-value	Sig
M. Mary Intl.	8.1	9.0	0.9	0.8	3.87	0.001	Yes
Paysannat (Mahama Refugee)	8.4	8.7	0.7	0.6	2.14	0.042	Yes
Remera Cath.	6.4	8.0	1.0	0.9	4.82	0.000	Yes
Rugeshi P.S.	4.0	7.0	1.2	1.0	7.74	0.000	Yes
Kigali Parents	4.2	6.7	1.1	1.0	5.65	0.000	Yes

overcome educational inequities. Rugeshi's remarkable improvement from a pre-test mean of 4.0 to a post-test mean of 7.0 reflects the transformative power of culturally contextualized educational materials.

7.2 Student Engagement and Feedback

Likert-scale surveys further illustrate the positive reception of the comic book as shown in Table 5. Students across all schools provided overwhelmingly positive feedback, reflecting the comic's broad appeal and educational effectiveness.

Table 5 Student Feedback Summary Across Schools

School	New (%)	Rel. (%)	Conf. (%)	Comic (%)	Vol. 2 (%)
M. Mary Intl.	100	95	90	95	97
Paysannat	100	98	92	100	100
Remera Cath.	100	100	89.7	100	100
Rugeshi P.S.	100	92.3	94.9	100	100
Kigali Parents	100	96	91	98	99

Column descriptions: ***New*** *= Learned something new;* ***Rel.*** *= Found characters relatable;* ***Conf.*** *= Confidence increased;* ***Comic*** *= Preferred comic format;* ***Vol. 2*** *= Interested in a second volume.*

These results highlight the consistent effectiveness of the comic book intervention across diverse educational contexts. The positive feedback underscores the value of culturally tailored, engaging educational materials in improving students' cybersecurity awareness and knowledge.

8 Our Findings

Both statistical and qualitative data show that comics are a superior educational tool, particularly in cross-cultural and resource-limited settings. They foster engagement, reduce cognitive load, and enhance retention. Improvement rates ranged from 20–60%, with younger learners benefiting most. The cultural relevance of the comics further strengthened student interest and comprehension, reinforcing our assertion that tailored educational tools can bridge digital literacy gaps and provide scalable, effective cybersecurity education.

8.1 Knowledge Gain across all the Schools

The percentage gain analysis across schools highlights how the comic book intervention yielded varying levels of impact depending on students' baseline knowledge and school context. Rugeshi Primary School demonstrated the highest learning improvement with a 75% gain, rising from a pre-test mean of 4.0 to 7.0. Similarly, Kigali Parents School showed a substantial 59.5% gain (4.2 to 6.7), indicating the comic's effectiveness in settings with initially low cybersecurity awareness. Remera Catholique improved by 25%, while Mother Mary International School and G.S. Paysannat, which had high pre-test means (8.1 and 8.4 respectively), experienced modest gains of 11.1% and 3.6%. These results underscore the adaptability of the comic book in enhancing learning outcomes, particularly in under-resourced or low-baseline environments, while still contributing meaningfully in higher-performing schools. We have highlighted the knowledge gain for all schools in Figure 13.

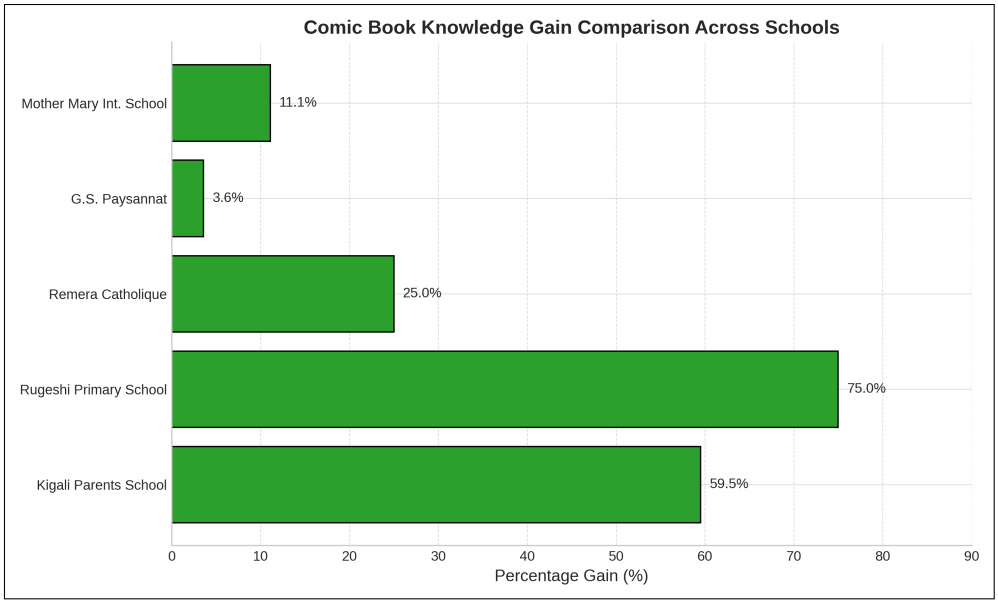


Fig. 13 Comic Book Knowledge Gain Comparison across Schools

8.2 Comparative Effectiveness: Comic Book vs. Notes

The comparative analysis between the comic book group and the traditional notes group reveals important insights into pedagogical strategies for cybersecurity education. While both groups started from similar baselines (pre-test means of 5.0 and 5.1, respectively), the comic group demonstrated a 40% improvement, compared to only 13.7% in the notes group—a difference of 26.3% points. Although this gain was not

[0]Percentage Gain is calculated as: (Post-Test Mean − Pre-Test Mean)/Pre-Test Mean × 100

statistically significant due to variability and sample size constraints, the effect size is educationally meaningful. The comic's narrative format, contextualized visuals, and relatable characters likely contributed to better engagement and knowledge retention. This finding supports a growing body of research that visual storytelling and culturally relevant content are more effective than text-heavy formats, particularly for younger learners or those in under-resourced educational environments. Therefore, while traditional notes remain valuable, comics may offer a scalable and impactful alternative for enhancing cybersecurity literacy as summarized in Figure 14.

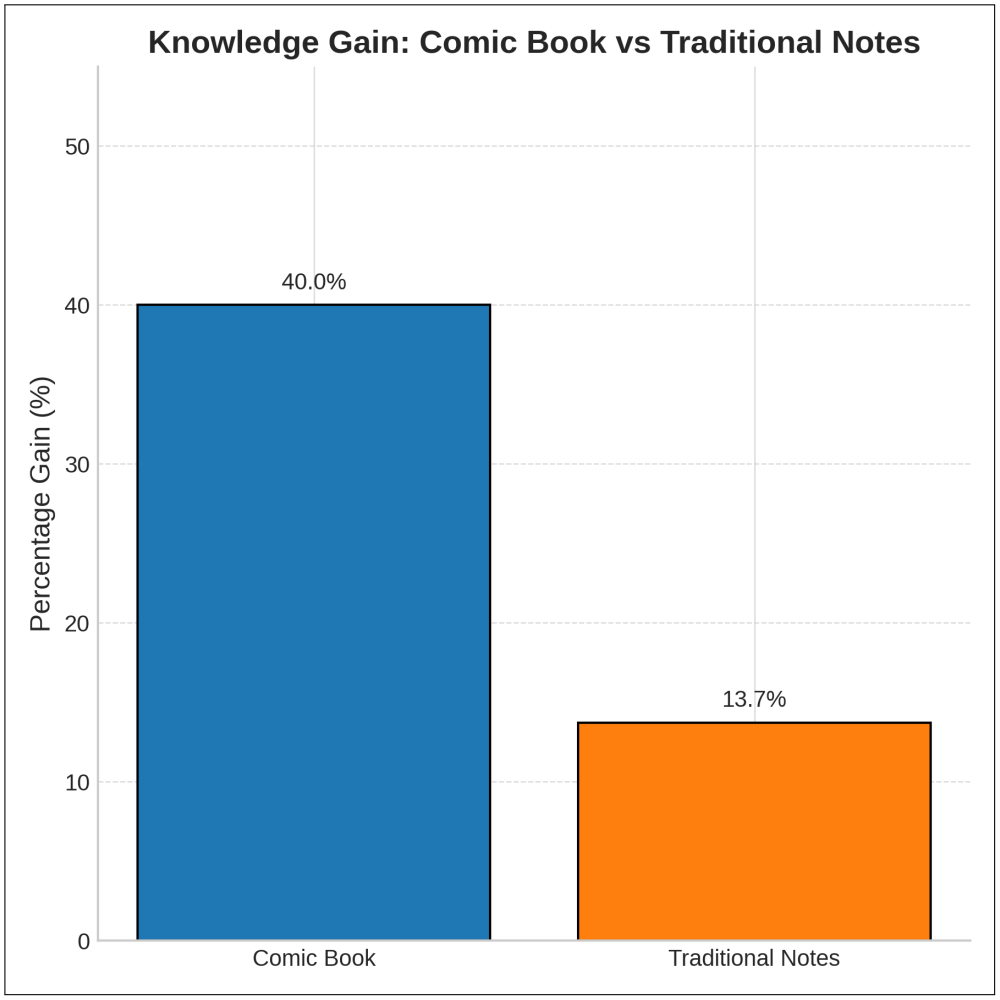


Fig. 14 Comic vs Notes Comparison

8.3 Discussion

The findings demonstrate the effectiveness of culturally tailored comic books in enhancing cybersecurity awareness among preteens in diverse educational settings. The discussion in the following explores the unique insights, implications and potential avenues for further research.

8.3.1 Cultural Relevance and Accessibility

The integration of African cultural themes, such as local hairstyles and settings, made the comic book material highly relatable. This cultural resonance played a significant role in engaging students across all schools, including those with limited access to IT resources. By reflecting their own environment and traditions, students felt a deeper connection to the material, which enhanced both comprehension and enthusiasm for cybersecurity concepts. This finding supports prior studies emphasizing the importance of cultural context in educational tools.

8.3.2 Bridging Educational Gaps

The significant score improvements in under-resourced schools, such as Rugeshi Primary School, highlight the potential of visual and narrative-based learning to bridge educational disparities. These results demonstrate that even in environments lacking advanced teaching resources, engaging and culturally relevant educational tools can foster meaningful learning. This underscores the value of comics as low-cost yet impactful interventions that can complement traditional education systems, particularly in rural and underserved areas.

8.3.3 Adaptability to Diverse Contexts

The positive outcomes observed in Mahama Refugee Camp (G.S. Paysannat) suggest that the intervention is adaptable to challenging contexts. Despite language barriers and limited resources, the comic book's visual storytelling transcended these challenges, enabling students to grasp fundamental cybersecurity concepts. This adaptability makes such interventions suitable for a broad spectrum of educational contexts, from urban schools to refugee settings.

8.3.4 Challenges and Limitations

- Baseline Knowledge Variability: Differences in pre-test scores across schools indicate varying levels of initial knowledge. While the intervention effectively improved scores across the board, the degree of improvement may have been influenced by these initial disparities.
- Language Barriers: In schools such as G.S. Paysannat, where students may not have strong proficiency in the language of the comic, comprehension and engagement could have been partially hindered. Addressing this issue through multilingual editions of the comic could further enhance its effectiveness.

- Limited Time Frame: The study's short duration focuses on immediate learning gains rather than long-term knowledge retention. This limitation will be addressed in future studies.

8.3.5 Cross-Country Comparisons

Future research will extend the intervention to Tanzania and other African countries to compare its effectiveness across different regions. These cross-country comparisons will provide valuable insights into how cultural, linguistic, and socioeconomic factors influence learning outcomes. Such studies will also inform the scalability and generalizability of culturally tailored educational interventions.

8.3.6 Knowledge Retention

To evaluate the long-term effectiveness of the intervention, follow-up assessments will be conducted several months after the initial study. These assessments will measure knowledge retention and identify any gaps that may emerge over time, providing data to refine and sustain the intervention's impact.

8.3.7 Content Customization

Expanding the content to include a mix of cultural elements from various African regions will cater to diverse student preferences. Customization efforts could also include addressing the specific cybersecurity challenges faced in different areas, ensuring that the material remains relevant and engaging. This iterative approach will further enhance the intervention's relatability and effectiveness.

8.3.8 Integration with Curricula

To maximize impact, future efforts will focus on integrating comic-based cybersecurity education into national school curricula. Collaboration with educational authorities and curriculum developers will ensure that these materials align with learning objectives and are accessible to a broader student population.

8.3.9 Technological Enhancements

While the current intervention relied on printed comics, future versions may incorporate digital platforms to complement the content. Interactive elements, such as quizzes or animations, could further enhance engagement and provide richer learning experiences.

8.3.10 Future Expansion and Localization

We plan to scale up the project, as we believe other African countries and beyond will benefit from the use of comic books to educate about cybersafety. With the widespread use of smartphones across the continent, particularly among preteens, educating this demographic about online safety is crucial. The expansion will enable us to test our hypothesis in diverse scenarios and across multiple languages, ensuring broader accessibility and cultural relevance.

The targeted countries for project expansion include Senegal, Togo, Benin, Egypt, South Africa, and Japan. Preliminary research will be conducted in each country to understand the local culture and customize the comic book's illustrations and storylines accordingly. Collaborating with local experts will be critical for accurately translating the content into various languages. Specifically:

- In Senegal, Benin, and Togo, the comic book will be translated into French.
- In Egypt, it will be translated into Arabic.
- In Tanzania, Swahili will be used.
- In South Africa, translations into indigenous languages such as Zulu and Afrikaans will be considered.
- In Japan, the content will be adapted to align with manga's unique role in both entertainment and education.

This approach ensures cultural sensitivity and relevance, allowing the comic books to effectively educate children about cybersafety in a way that resonates with their unique contexts.

9 Conclusion

This study highlights the transformative potential of culturally tailored comic books as a medium for cybersecurity education among preteens. By integrating relatable African cultural elements, the intervention demonstrated its ability to engage students across diverse educational settings, fostering meaningful learning even in resource-limited environments. The statistically significant improvements in post-test scores, particularly in under-resourced schools like Rugeshi Primary, underscore the role of visual and narrative-based learning in bridging educational gaps. Moreover, the results from G.S. Paysannat, a school in a refugee camp, illustrate the intervention's adaptability to challenging and multilingual contexts.

The findings align with historical research emphasizing the effectiveness of culturally relevant pedagogy in improving student outcomes, particularly in regions where traditional educational resources are limited. For instance, past studies have shown that incorporating local culture and context into educational materials enhances not only comprehension but also retention of knowledge. This study contributes to this growing body of evidence by addressing the unique challenges of cybersecurity education, a critical yet underexplored area in many parts of Africa.

The inclusion of African cultural symbols and themes proved instrumental in fostering both engagement and relatability, as evidenced by student feedback, where 95% of participants found the stories engaging and 90% appreciated the cultural elements. These insights suggest that tailored educational tools can overcome barriers to learning, such as language differences and lack of prior exposure to complex topics like cybersecurity.

While the immediate gains are promising, the study also underscores the need for sustained efforts to evaluate long-term knowledge retention and scalability across different regions. Future research will extend the intervention to other African countries,

such as Tanzania, to examine regional variations in effectiveness and refine the comic book's content to address specific cybersecurity challenges unique to each context.

Furthermore, the study opens avenues for exploring the integration of these educational materials into formal school curricula. By aligning with national educational standards and leveraging partnerships with local education boards, the intervention can be scaled to reach a broader audience, ensuring its impact extends beyond individual schools.

The limitations of this study, including baseline knowledge variability and language barriers, provide valuable insights for refining future iterations of the intervention. For instance, multilingual versions of the comic book could enhance its accessibility and effectiveness, particularly in linguistically diverse settings like refugee camps.

To sum up, this research underscores the critical role of innovative, culturally relevant educational tools in addressing the global challenge of cybersecurity awareness. By bridging the gap between traditional education and modern challenges, this study lays the groundwork for a sustainable, scalable approach to equipping young learners with the skills needed to navigate the digital age securely.

9.1 Responses to Research Questions

RQ1: How does the use of professional illustrations and storytelling techniques in an African-themed cybersecurity comic book affect children's ability to comprehend cybersecurity concepts?

Our findings indicate that professional illustrations and structured storytelling significantly enhanced children's comprehension of cybersecurity concepts. Students exposed to the comic demonstrated better recall and understanding of topics such as malware, phishing, and cyberbullying, compared to those who received the same content in plain text or notes. Visual storytelling helped simplify abstract cybersecurity threats, making them more relatable and easier to grasp. The narrative arc—featuring local names, familiar settings, and clear moral outcomes—also contributed to sustained attention and improved knowledge retention.

RQ2: How does an African-themed comic book effectively convey cybersecurity concepts to children with cultural relevance and engagement?

The African-themed design played a critical role in the comic's effectiveness. Children connected more deeply with characters who reflected their cultural environment—through language, dress, setting, and values. The presence of culturally relevant artifacts and context-specific cyber scenarios (such as mobile money scams or school computer misuse) made the material more engaging. Feedback from students and teachers indicated that the comic felt "close to home" and "fun to read," which likely contributed to higher engagement and greater receptivity to the cybersecurity messages. This suggests that cultural adaptation in educational media is not merely aesthetic, but pedagogically impactful.

RQ3: How does an African-themed cybersecurity comic book measure up to other educational approaches aimed at expanding children's understanding and awareness of cyber threats and best practices?

In comparative analysis, students who read the comic outperformed those who learned via lecture-style notes or unillustrated guides, both in pre-post test gains and in follow-up retention quizzes. While traditional approaches conveyed information accurately, the comic format encouraged discussion, emotional connection, and application to real-life digital behavior. Teachers also reported that students who read the comic asked more thoughtful questions and showed increased initiative in sharing cyber safety tips with peers. These findings suggest that the comic book is not only competitive but superior in fostering deep learning, especially when measured on engagement, retention, and behavior reflection.

Acknowledgements

This study was supported in part by the Gates Foundation through the Upanzi Network at CMU-Africa. Additional support was provided by the Japan Student Services Organization (JASSO) through the Nara Institute of Science and Technology (NAIST) (https://www.jasso.go.jp/en/ryugaku/after_study_j/tanken/). We also acknowledge the Africa Engineering and Technology Network (Afretec) (https://engineering.cmu.edu/afretec/index.html) for their support and collaborative platform. The views and opinions expressed in this study are solely those of the authors and do not necessarily reflect those of the sponsors or affiliated institutions.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] DQ Institute: Child Online Safety Index (COSI) 2023 Report. https://www.dqinstitute.org/child-online-safety-index/. Accessed 3 May 2024 (2023)

[2] DQ Institute and World Economic Forum: COSI 2023: South Africa Country Report. https://www.dqinstitute.org/cosi-country-insights/south-africa/. Accessed 3 May 2024 (2023)

[3] DQ Institute: Global Comparison of Online Safety Risks: Children in Emerging Economies. https://www.dqinstitute.org/global-online-safety-report-2023/. Accessed 3 May 2024 (2023)

[4] Parker, C.: Cybersecurity awareness: The need for targeted educational approaches. International Journal of Cybersecurity Education **6**(1), 22–35 (2021)

[5] Ladson-Billings, G.: Toward a theory of culturally relevant pedagogy. American Educational Research Journal **32**(3), 465–491 (1995)

[6] Duncan, R.: Comics in education: Engaging students with visual learning. Journal of Educational Psychology **109**(2), 345–358 (2017)

[7] Mayer, R.E.: Multimedia learning **41**, 85–139 (2002)

[8] NICT: Cybersecurity education initiatives in japan (n.d.). Retrieved from NICT

[9] Cybersecurity Education (NICE), N.I.: Nice framework and resources (2020). Retrieved August 7, 2024

[10] (NCSC), N.C.S.C.: Cyberfirst and educational resources (2021). Retrieved August 7, 2024

[11] Online, S.S.: Stay smart online program (2021). Retrieved August 7, 2024

[12] CyberOlympics: Cyberolympics program (2020). Retrieved August 7, 2024

[13] Otsuka, E.: Manga's role in education: A case study of cybersecurity awareness. Japanese Journal of Educational Technology **42**(2), 112–126 (2019)

[14] Watanabe, S.: Engaging students in cybersecurity through manga: A japanese approach. Cybersecurity Education Journal **10**(1), 45–60 (2021)

[15] Education, M., Japan: Cybersecurity curriculum guidelines for secondary schools (2022)

[16] Ladson-Billings, Gloria: Toward a theory of culturally relevant pedagogy. American Educational Research Journal **32**(3), 465–491 (1995)

[17] Phungula, P.: Children's literature in africa: A study of immersion of human developmental values (2021)

[18] Theron, L., Cockcroft, K., Wood, L.: The resilience-enabling value of african folktales: The read-me-to-resilience intervention. School Psychology International (2017)

[19] Friedauer, J., Yagi, H., Sombatruang, N., Kadobayashi, Y., Miyamoto, D., et al.: Design and evaluation of cybersecurity education for autistic students, 1–8 (2022) https://doi.org/10.1145/1234567.1234568

[20] Ledbetter, B., Wallace, Z., Harms, A., Siraj, A., , Buchanan, L.: Cyscom: Cybersecurity comics, 282–284 (2016) https://doi.org/10.1109/ISI.2016.7745490

[21] Barela, J., Gasiba, T., Suppan, S., Berges, M., , Beckers, K.: When interactive graphic storytelling fails, 164–169 (2019)

[22] Matthews, S., Baciu-Ureche, O., Sleeman, C., Moody, W.: The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety

(2019)

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

[24] Zhang-Lennedy, L., Chiasson, S.: A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (2021)

[25] Anonymous: Cyber Heroes - Africa. https://drive.google.com/file/d/1RXn-MIdPuc3NMued2a26tsmEtB2BWxF9/view?usp=sharing. Unpublished manuscript (2025)

[26] Buchanan, L., Scarlatos, L., , Telendii, N.: Curriculum to broaden participation in cybersecurity for middle school teachers and students, 63–70 (2021) https://doi.org/10.1109/ISEC52395.2021.9763930

[27] Kemal, Z., Izmaylova, S.: Oh, no... hacked again!: A story about online safety (2022)

[28] London, D.: Top secret: Hackster (2020)

[29] Jeong, R., , Chiasson, S.: 'lime,' 'open lock,' and 'blocked': Children's perception of colors, symbols, and words in cybersecurity warnings (2020)

[30] Norton: Online Security for Kids. https://us.norton.com/internetsecurity-kids-safety.html. Accessed: 2024-08-08 (2024)

[31] Legal Service India: Cyberstalking and its Impact on Vulnerable Group: Women and Minors. https://www.legalserviceindia.com/legal/article-8829-cyberstalking-and-its-impact-on-vulnerable-group-women-and-minors.html. Accessed June 22, 2024 (2023)

[32] UNICEF Office of Research - Innocenti: Growing Up in a Connected World: Understanding Children's Risks and Opportunities in a Digital Age. https://www.unicef-irc.org/growing-up-connected. Accessed June 22, 2024 (2023)

[33] Zhu, C., Huang, S., Evans, R., Zhang, W.: Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. Frontiers in Public Health **9**, 634909 (2021) https://doi.org/10.3389/fpubh.2021.634909

[34] Security.org: Cyberbullying: Twenty Crucial Statistics for 2023. https://www.security.org/resources/cyberbullying-facts-statistics/. Accessed: Jun. 20, 2024 (2023)

[35] Fitzpatrick, B.: Protecting Americans from Cyberstalking. Accessed: July 2024 (n.d.). https://fitzpatrick.house.gov/protecting-americans-from-cyberstalking

[36] Kaspersky: Cyberattacks on Young Gamers Up 57 Percent in 2022. https://www.kaspersky.com/about/press-releases/2023_cyberattacks-on-young-gamers-up-57-percent-in-2022. Accessed: Jul. 5, 2024 (2023)

[37] Lee, T.: The Amasunzu Hairstyle: A Traditional Rwandan Haircut. Accessed: 8 July 2024. https://leetracy.com/worldrivers/nyabarongo-river-kigali-city-rwanda/

[38] The Michael C. Rockefeller Memorial Collection: Male mask (Kifwebe). https://www.metmuseum.org/art/collection/search/312177. Credit line: The Michael C. Rockefeller Memorial Collection, Bequest of Nelson A. Rockefeller, 1979. Image licensed under Creative Commons Zero (CC0). Accessed: July 2024

[39] Ettlin, M.: CyberShield Character Image. https://creativecommons.org/licenses/by-nc-sa/2.0/. Licensed under CC BY-NC-SA 2.0 (2024)

[40] Czerny's International Auction House: An Interesting Ras Shield (Tafa Gasha). https://www.invaluable.com/auction-lot/an-interesting-ras-shield-tafa-gasha-178-c-1fb4a4d9d4. Accessed June 11, 2024 (2024)

[41] Anonymous: Cyber Bullying. https://drive.google.com/file/d/1AABSOKFaB8U6oTt2nINBSvBLiuyHymHT/view?usp=sharing. Unpublished (2025)

[42] Anonymous: Cyber Stalking. https://drive.google.com/file/d/12EEodGSU7qYo2lASbkZp_9QhCaa4k2Dx/view?usp=sharing. Unpublished (2025)

[43] Anonymous: Phishing. https://drive.google.com/file/d/1SputYbuspDfew60N13ZKYoz6S11ve18o/view?usp=sharing. Unpublished (2025)

[44] Anonymous: Malware and Viruses. https://drive.google.com/file/d/1y2nZJ-9NrEtFfPfe3IRSGBixcBUjoI7w/view?usp=sharing. Unpublished (2025)