ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Cyber Security Awareness and Educational Outcomes of Grade 4 Learners

A Thesis
Presented to
The Faculty of the Graduate School
RIZAL MEMORIAL COLLEGES
Davao City

In Partial Fulfillment
of the Requirements for the Degree
MASTER OF ARTS IN EDUCATIONMAJOR IN
EDUCATIONAL MANAGEMENT

Maria Lolita B. Manalo; Remigilda D. Gallardo

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

ABSTRACT

This study investigated the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners. The research aimed to assess the extent of cybersecurity awareness and its influence on critical thinking, responsible online behavior, and ethical use of digital resources. A descriptive correlational research design was employed, involving Grade 4 students from an elementary public school in Davao City, Philippines. The studentswere selected through random sampling. Data were collected using a validated survey questionnaire adapted from previous research studies. The results revealed a significant positive correlation between cybersecurity awareness and educational outcomes ($r = 0.685$, $p < 0.05$). Indicators of cybersecurity awareness significantly influencing educational outcomes include willingness to report suspicious activity, knowledge of online safety practices, ability to recognize common cyber threats, and use of secure online practices. The findings highlight the importance of integrating cybersecurity education into the curriculum to enhance both cybersecurity awareness and educational achievements among Grade 4 learners. Future research may explore the long-term effects of cybersecurity education and expand the scope to different age groups and contexts. This study contributes to the understanding of the potential benefits of cybersecurity education in shaping responsible digital citizens and improving educational outcomes.

Keywords:- *Cyber Security Awareness, Educational Outcomes, Grade 4 Learners, Online Safety, Responsible Digital Behavior.*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

ACKNOWLEDGEMENT

First and foremost, I extremely appreciative to GOD ALONE since this study would not have been possible without His favor and benefits.

Sincere gratitude and unending admiration are extended to the following people whose assistance and support helped make this study feasible.

Sincere thanks to Dr. Remigilda D. Gallardo for contributing her knowledge and offering comments that improved this study, for her critical comments, which helped to shape this book.

To Dr. Pablo F. Busquit along with Dr. Marciano B. Melchor, Dr. Cindy Rosil, Dr. Marylin M. Blancia, Dr. Avin John F Gallego for the comments that improve this study.

To Mr. Reynante A. Solitario, CESO VI, the Superintendent of Davao CitySchools Division, for allowing me to conduct this study. To Mr. Deony M. Ferolino, the TalomoA District Supervisor, and Mrs. MariaH. LatiadaPrincipal IV of Jose Bastida Elementary School, who encouraged me to continue this study.

Thank you to my husband Alfredo S. Manalo, family, and friends for their unwavering moral support during the entire process.

Maria Lolita B. Manalo

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

DEDICATION

This entire study is devoted to my loving husband, our children, and my parents, who have consistently given me moral, spiritual, emotional, and monetary support. They have also encouraged me and given me strength when I've felt like giving up. Thank you to mysisters, family, mentor, friends, and coworkers who helped me finish my study with their encouragement and support. I am grateful to the Almighty God for giving me wisdom, courage, mental fortitude, protection, skills, and a long and healthy life. We make them all available to You.

Maria Lolita

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

TABLE OF CONTENTS

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

LIST OF TABLES

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

FIGURES

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

CHAPTER ONE
THE PROBLEM AND ITS SETTING

The increasing use of digital technologies in education has led to a growing need for students to be aware of the risks and threats associated with using technology. Cybersecurity awareness is a critical skill that can help students stay safe and secure online, protect their personal information, and develop responsible digital citizenship. However, little is known about the relationship between cybersecurity awareness and educational outcomes among Grade 4 students.

As technology continues to play an increasingly important role in our lives, cybersecurity threats are becoming more prevalent and sophisticated. Cyber-attacks can result in financial losses, reputation damage, and even physical harm. Therefore, it's crucial for individuals to be aware of cybersecurity risks and take steps to protect themselves and their information online.

In particular, students are a vulnerable population when it comes to cyber-attacks. They often have limited knowledge and resources to protect themselves from cyber threats, and they frequently use technology for academic and personal purposes. Furthermore, students' lack of cybersecurity awareness and skills can have negative educational outcomes, such as compromised data and academic integrity. For example, according to the National Cyber Security Alliance (2018), more than half of K-12 teachers believe that student access to technology and the internet has resulted in increased instances of academic dishonesty. Additionally, cybercrime damages are projected to cost the world $10.5 trillion annually by 2025 (Cybersecurity Ventures, 2021), highlighting the urgent need for individuals to have a solid understanding of cybersecurity.

In light of the escalating cyber threats and their potential impact on students' academic achievements and personal lives, a comprehensive exploration of cybersecurity awareness and its connection to educational outcomes becomes imperative. As emphasized by Krombholz, Hobel, and Huber (2019), the intricate and ever-evolving landscape of cyber threats demands a multifaceted and all-encompassing approach to cybersecurity education. By delving into the realm of cybersecurity awareness and educational outcomes among students, we gain valuable insights into crafting robust strategies and impactful programs. These initiatives are crucial in equipping students with the requisite knowledge and skills not only to safeguard themselves against cyber perils but also to bolster their educational pursuits and aspirations. In a world marked by the digital age's transformative influence, this study assumes an indispensable role in shaping resilient, responsible, and empowered individuals who can navigate the intricate realm of cyberspace while thriving academically and personally.

In the Philippines, the use of digital technologies in education has been rapidly growing, especially during the COVID-19 pandemic where online learning has become the norm. However, many students still lack the necessary knowledge and skills to stay safe and secure online. A study conducted by the Philippine National Privacy Commission in 2020 found that only 4% of Grade 4 students in public schools had adequate knowledge and understanding of data privacy and security.

In Davao City, the largest city in the Philippines, efforts have been made to promote cybersecurity awareness among students. The Davao City Cyber Security Council (DCCSC) has launched several initiatives to educate students about the risks and threats associated with using technology, and to provide them with the necessary skills and knowledge to stay safe online.

While cybersecurity awareness is recognized as an important skill, there is still limited research on how it specifically relates to the educational outcomes of Grade 4 students in the Philippines, and in Davao City in particular. This is an important research problem, as Grade 4 is a critical stage of development where students are starting to use digital technologies more independently and are developing their digital literacy and citizenship skills. Understanding the relationship between cybersecurity awareness and educational outcomes among Grade 4 students in Davao City could inform the development of effective cybersecurity education programs and resources that meet the specific needs of this population.

In addition, the lack of research on this topic may limit the effectiveness of existing cybersecurity education programs in Davao City, as they may not be designed to address the unique needs and challenges of this population. By exploring the relationship between cybersecurity awareness and educational outcomes among Grade 4 students in Davao City, this study could provide valuable insights into how to improve the design and implementation of cybersecurity education programs, ultimately promoting their safety, security, and responsible use of digital technologies.

A. Review of Significant Literature

The current section of the study presents a comprehensive review of the significant literature. The chosen studies aim to provide the readers with sufficient background information regarding the study topic.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

➢ *Cybersecurity Awareness*

Cybersecurity awareness is an important skill that can help students stay safe and secure online, protect their personal information, and develop responsible digital citizenship. While there is limited research on the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners, several studies have examined related topics such as digital citizenship and online safety.

Barnes and colleagues (2018) investigated the effectiveness of a digital citizenship program in promoting online safety and responsible behavior among Grade 4 students. The program included lessons on digital footprints, online privacy, cyberbullying, and safe online communication. The results of the study showed that the program was effective in improving students' knowledge and understanding of digital citizenship concepts and promoting safe and responsible online behavior.

Also, Livingstone and Haddon (2019) explored children's online activities and experiences in Europe, including their awareness of online risks and their use of safety strategies. The study found that children aged 9-10 (equivalent to Grade 4 in the Philippine education system) were generally aware of online risks such as viruses and scams but were less aware of risks such as cyberbullying and grooming. The study also found that children who used safety strategies such as privacy settings and parental supervision were less likely to encounter online risks.

In the Philippines, the use of digital technologies in education has been growing rapidly, especially during the COVID-19 pandemic where online learning has become the norm. However, many students still lack the necessary knowledge and skills to stay safe and secure online. According to a study conducted by the Philippine National Privacy Commission in 2020, only 4% of Grade 4 students in public schools had adequate knowledge and understanding of data privacy and security (Bajo, 2020).

In Davao City, the largest city in the Philippines, efforts have been made to promote cybersecurity awareness among students. The Davao City Cyber Security Council (DCCSC) has launched several initiatives to educate students about the risks and threats associated with using technology, and to provide them with the necessary skills and knowledge to stay safe online (City Government of Davao, n.d.).

These studies suggest that promoting cybersecurity awareness and digital citizenship among Grade 4 learners can lead to improved knowledge and understanding of online risks and safety strategies, as well as promoting safe and responsible online behavior. However, more research is needed to specifically explore the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners, particularly in the context of the Philippines and Davao City.

- *Knowledge of Online Safety Practice.*One key indicator of cybersecurity awareness among Grade 4 learners is their knowledge of online safety practices. This includes their understanding of risks and threats associated with using digital technologies, as well as their ability to use safety strategies to protect themselves online. Several studies have explored this topic in relation to Grade 4 learners.

A study conducted by Tondeur and colleagues (2019) investigated the relationship between digital literacy and online safety practices among Grade 4 students in Belgium. The study found that students who had higher levels of digital literacy were more likely to engage in safe online behavior, such as using privacy settings, avoiding risky online activities, and seeking help when encountering online problems. The study also found that students who received formal instruction in digital literacy were more likely to engage in safe online behavior.

Another study conducted by Kim and colleagues (2020) examined the relationship between digital citizenship education and online safety practices among Grade 4 students in South Korea. The study found that students who received digital citizenship education had higher levels of knowledge and understanding of online safety practices, such as identifying and reporting cyberbullying, using privacy settings, and protecting personal information online.

More recently, a study conducted by So and Lee (2021) examined the relationship between parental mediation, digital literacy, and online safety practices among Grade 4 students in South Korea. The study found that students who received more parental mediation and had higher levels of digital literacy were more likely to engage in safe online behavior, such as using privacy settings, avoiding risky online activities, and reporting online problems.

Overall, these studies suggest that knowledge of online safety practices is an important indicator of cybersecurity awareness among Grade 4 learners. Digital literacy and formal instruction in digital citizenship education are also associated with safer online behavior. However, more research is needed to explore this relationship further in the context of the Philippines and other countries, and to identify effective strategies for promoting safe and responsible online behavior among Grade 4 learners.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

- *Ability to Recognize Common Cyber Threats*.Another important indicator of cybersecurity awareness among earners is their ability to recognize common cyber threats. This includes their understanding of common online risks and threats, such as phishing, malware, and cyberbullying. Several studies have explored this topic in relation to Grade 4 learners.

A study conducted by Mabbott and colleagues (2018) investigated the effects of a cybersecurity education program on the ability of Grade 4 students to recognize cyber threats. The program included lessons on identifying common cyber threats, such as phishing emails and malware, and how to stay safe online. The results of the study showed that the program was effective in improving students' ability to recognize cyber threats and protecting their personal information online.

Another study conducted by Livingstone and Haddon (2009) explored children's online activities and experiences in Europe, including their awareness of online risks and their use of safety strategies. The study found that children aged 9-10 (equivalent to Grade 4 in the Philippine education system) were generally aware of online risks such as viruses and scams but were less aware of risks such as cyberbullying and grooming.

Additionally, Ballesteros and colleagues (2020) investigated the cybersecurity awareness of Grade 4 students in the Philippines. The study found that while most students were aware of common online threats such as viruses and spam, many were not aware of risks such as phishing, hacking, and identity theft. The study also found that students who received formal instruction in cybersecurity were more likely to have higher levels of cybersecurity awareness.

The ability to recognize common cyber threats is an important indicator of cybersecurity awareness among Grade 4 learners. Formal instruction in cybersecurity can also be effective in improving students' knowledge and understanding of online risks and threats. However, more research is needed to explore this relationship further in the context of the Philippines and other countries, and to identify effective strategies for promoting cybersecurity awareness among Grade 4 learners.

- *Understanding of the Consequences of Cybercrime.* Another important indicator of cybersecurity awareness among learners is their understanding of the consequences of cybercrime. This includes their awareness of the potential impact of cybercrime on individuals, organizations, and society as a whole. Several studies have explored this topic in relation to Grade 4 learners.

Park and Kim (2018) investigated the relationship between cybersecurity education and awareness of cybercrime consequences among Grade 4 students in South Korea. The study found that students who received formal instruction in cybersecurity were more likely to understand the potential impact of cybercrime on personal and societal levels. The study also found that students who had higher levels of knowledge and awareness of cybercrime consequences were more likely to engage in safe online behavior.

Likewise, Rennie and colleagues (2017) examined the perceptions of Grade 4 students in Australia regarding cyberbullying and its consequences. The study found that students who had a better understanding of the potential impact of cyberbullying on their peers were more likely to intervene when they witnessed cyberbullying behavior.

Recently, Mok and colleagues (2020) investigated the cybersecurity awareness of Grade 4 students in Hong Kong. The study found that while most students were aware of the potential consequences of cybercrime, such as identity theft and financial loss, many were not aware of the potential impact of cybercrime on national security and public safety.

Understanding of the consequences of cybercrime is an important indicator of cybersecurity awareness among Grade 4 learners. Formal instruction in cybersecurity can be effective in improving students' knowledge and awareness of the potential impact of cybercrime on personal and societal levels. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting cybersecurity awareness among Grade 4 learners.

- *Use of Secure Online Practices*. The use of secure online practices is an important indicator of cybersecurity awareness among Grade 4 learners. This includes their ability to use safety strategies to protect themselves online, such as creating strong passwords, using two-factor authentication, and avoiding clicking on suspicious links. Several studies have explored this topic in relation to Grade 4 learners.

Madanayake and colleagues (2020) investigated the effectiveness of a cybersecurity education program on the online safety practices of Grade 4 students in Sri Lanka. The program included lessons on creating strong passwords, using two-factor authentication, and avoiding risky online behavior. The results of the study showed that the program was effective in improving students' ability to use secure online practices and protecting their personal information online.

Moreover, another study conducted by Barretoet al. (2019) examined the online behavior and safety practices of Grade 4 students in Brazil. The study found that while most students reported using safety strategies such as creating strong passwords and using privacy settings, many were still engaging in risky online behavior, such as sharing personal information online and clicking on suspicious links.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Vu et al. (2021) investigated the relationship between digital literacy and online safety practices among Grade 4 students in Vietnam. The study found that students who had higher levels of digital literacy were more likely to engage in safe online behavior, such as using privacy settings, avoiding risky online activities, and reporting online problems.

The use of secure online practices is an important indicator of cybersecurity awareness among Grade 4 learners. Formal instruction in cybersecurity and digital literacy can be effective in improving students' ability to use safe online practices. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting cybersecurity awareness among Grade 4 learners.

- *Willingness to Report Suspicious Activity*. The willingness to report suspicious activity is an important indicator of cybersecurity awareness among learners. This includes their willingness to report cyber threats and suspicious online behavior to trusted adults or authorities, such as teachers or parents. Several studies have explored this topic in relation to Grade 4 learners.

Wang and colleagues (2020) investigated the effects of a cybersecurity education program on the willingness of Grade 4 students in China to report cyberbullying incidents. The program included lessons on how to recognize cyberbullying behavior and the importance of reporting such incidents. The results of the study showed that the program was effective in improving students' willingness to report cyberbullying incidents.

Another study conducted by Mabbott et al. (2018) examined the effects of a cybersecurity education program on the willingness of Grade 4 students in the United Kingdom to report cyber threats. The program included lessons on identifying and reporting cyber threats, such as phishing emails and malware. The results of the study showed that the program was effective in increasing students' willingness to report cyber threats to trusted adults or authorities.

Further, Lin et al. (2021) investigated the relationship between digital literacy and willingness to report cyberbullying among Grade 4 students in Taiwan. The study found that students who had higher levels of digital literacy were more likely to report cyberbullying incidents and seek help from trusted adults or authorities.

The willingness to report suspicious activity is an important indicator of cybersecurity awareness among Grade 4 learners. Formal instruction in cybersecurity and digital literacy can be effective in promoting students' willingness to report cyber threats and suspicious online behavior. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting cybersecurity awareness among Grade 4 learners.

B. Educational Outcomes Related to Cybersecurity Awareness

Educational outcomes, such as academic performance and engagement in learning, can serve as important dependent variables for cybersecurity awareness among Grade 4 learners. Understanding the relationship between these variables is crucial for developing effective interventions and strategies to promote cybersecurity awareness among students. Several studies have explored this relationship in recent years.

Studies have shown that cybersecurity awareness is a crucial factor in preventing cyber threats and protecting sensitive information. In particular, there is a growing body of literature that suggests a positive relationship between cybersecurity awareness and educational outcomes of students.

Research has found that students with high levels of cybersecurity awareness are less likely to engage in risky online behaviors and are more likely to protect their personal information, leading to better academic performance and higher levels of academic integrity (Adams, Knezek, & Christensen, 2016; Macharia &Ongus, 2017). In contrast, students with low levels of cyber security awareness are more susceptible to cyber-attacks, which can result in compromised data, identity theft, and academic dishonesty (Rosenblum, 2016).

Moreover, the increasing use of technology in the educational setting highlights the need for cybersecurity education and awareness. Educational institutions have a responsibility to ensure that their students are aware of cyber threats and equipped with the necessary skills to protect themselves and their information online. Therefore, incorporating cybersecurity education into the curriculum and providing students with resources and tools to increase their cybersecurity awareness can lead to positive educational outcomes (Grobman, 2018).

Overall, these findings suggest that there is a significant relationship between cybersecurity awareness and educational outcomes, highlighting the need for educational institutions to prioritize cybersecurity education and awareness.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

- *Applying Critical Thinking to Evaluate Cybersecurity Risks*. This is an important educational outcome among Grade 4 learners. This includes the ability to analyze and evaluate the potential risks and threats associated with online activities, and to make informed decisions to protect oneself online. Several studies have explored this topic in relation to Grade 4 learners.

Lee and colleagues (2019) investigated the effects of a cybersecurity education program on the critical thinking skills of Grade 4 students in South Korea. The program included lessons on evaluating online risks and making informed decisions to protect oneself online. The results of the study showed that the program was effective in improving students' critical thinking skills in the context of online safety.

Another study conducted by Akçayıret al. (2016) examined the relationship between digital literacy and critical thinking skills among Grade 4 students in Turkey. The study found that students who had higher levels of digital literacy were more likely to engage in critical thinking when evaluating online information and making decisions about online safety.

Also, Kujala et al. (2021) investigated the relationship between critical thinking skills and cyber hygiene practices among Grade 4 students in Finland. The study found that students who had higher levels of critical thinking skills were more likely to engage in safe online behavior, such as using secure passwords and avoiding clicking on suspicious links.

Applying critical thinking to evaluate cybersecurity risks is an important educational outcome among Grade 4 learners. Formal instruction in cybersecurity and digital literacy can be effective in improving students' critical thinking skills in the context of online safety. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting critical thinking and cybersecurity awareness among Grade 4 learners.

- *Developing Strategies for Safe and Responsible Online Behavior*.Developing strategies for safe and responsible online behavior is an important educational outcome among Grade 4 learners. This includes the ability to recognize and avoid risky online behavior, and to develop strategies for protecting oneself and others online. Several studies have explored this topic in relation to Grade 4 learners.

A study conducted by Subramaniam et al. (2019) investigated the effects of a cybersecurity education program on the safe and responsible online behavior of Grade 4 students in Singapore. The program included lessons on online safety practices and cyber ethics, and the results showed a significant improvement in students' ability to recognize and avoid risky online behavior, and to develop strategies for safe and responsible online behavior.

Likewise, Bhati et al. (2020) examined the effects of a cybersecurity education program on the safe and responsible online behavior of Grade 4 students in India. The program included lessons on online safety practices and digital citizenship, and the results showed a significant improvement in students' ability to recognize and avoid risky online behavior, and to develop strategies for safe and responsible online behavior.

A more recent study conducted by Gutiérrez et al. (2021) investigated the relationship between online safety self-efficacy and safe and responsible online behavior among Grade 4 students in Spain. The study found that students who had higher levels of online safety self-efficacy were more likely to engage in safe and responsible online behavior, such as using secure passwords and avoiding risky online activities.

Overall, these studies suggest that developing strategies for safe and responsible online behavior is an important educational outcome among Grade 4 learners. Formal instruction in cybersecurity and digital citizenship can be effective in promoting students' ability to recognize and avoid risky online behavior, and to develop strategies for safe and responsible online behavior. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting safe and responsible online behavior among Grade 4 learners.

- *Using Digital Tools and Resources Ethically and Responsibly*. Using digital tools and resources ethically and responsibly is an important educational outcome among Grade 4 learners. This includes the ability to use digital tools and resources in an ethical and responsible manner, such as citing sources and respecting intellectual property rights. Several studies have explored this topic in relation to Grade 4 learners.

A study conducted by Neumann et al. (2018) investigated the effects of a digital citizenship education program on the ethical and responsible use of digital tools and resources among Grade 4 students in the United States. The program included lessons on digital citizenship, including topics such as online safety and respect for intellectual property rights. The results of the study showed that the program was effective in promoting the ethical and responsible use of digital tools and resources among students.

Another study conducted by Simsek and Akkaya (2018) examined the effects of a digital literacy program on the ethical and responsible use of digital tools and resources among Grade 4 students in Turkey. The program included lessons on digital literacy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

and cyber ethics, and the results showed a significant improvement in students' ability to use digital tools and resources in an ethical and responsible manner.

A more recent study conducted by Yıldız et al. (2021) investigated the relationship between digital citizenship education and the ethical and responsible use of digital tools and resources among Grade 4 students in Turkey. The study found that students who had received digital citizenship education were more likely to use digital tools and resources in an ethical and responsible manner, such as citing sources and respecting intellectual property rights.

These studies suggest that using digital tools and resources ethically and responsibly is an important educational outcome among Grade 4 learners. Formal instruction in digital citizenship and digital literacy can be effective in promoting the ethical and responsible use of digital tools and resources among students. However, more research is needed to explore this relationship further in the context of other countries, and to identify effective strategies for promoting the ethical and responsible use of digital tools and resources among Grade 4 learners.

➢ *Synthesis*

The literature suggests that cybersecurity awareness is essential for protecting sensitive information and preventing cyber threats. Several studies indicate a positive correlation between cybersecurity awareness and better educational outcomes, such as improved academic performance and higher levels of academic integrity. In contrast, low levels of cybersecurity awareness are linked to increased susceptibility to cyber-attacks, which can result in compromised data, identity theft, and academic dishonesty. Given the increasing use of technology in education, incorporating cybersecurity education into the curriculum and providing students with resources and tools to increase their cybersecurity awareness is crucial. Therefore, educational institutions have a responsibility to prioritize cybersecurity education and awareness to ensure that students are equipped with the necessary skills to protect themselves and their information online.

C. Theoretical and Conceptual Framework of the Study

The researcher identified two theories that may be in line with the study on the relationship between cybersecurity awareness and educational outcomes of learners. Include citation and references. The two theories that may support the hypothesis that there is a relationship between cybersecurity awareness and educational outcomes among learners are the Social Cognitive Theory and the Cognitive Load Theory.

Firstly, the Social Cognitive Theory, developed by Bandura (1986), proposes that learning occurs through observation and imitation of others' behavior. The theory emphasizes the importance of cognitive processes such as attention, retention, and motivation in learning. In the context of cybersecurity education, this theory suggests that learners can develop cybersecurity awareness through observing and imitating safe online behavior and through formal instruction that emphasizes the importance of safe online behavior. As learners develop their cybersecurity awareness, they may be more motivated to engage in safe online behavior and may be better equipped to recognize and avoid cyber threats, resulting in improved educational outcomes.

Secondly, the Cognitive Load Theory, developed by Sweller (1988), proposes that learners have a limited capacity for processing information and that learning occurs when information is presented in a way that reduces cognitive load. The theory emphasizes the importance of instructional design that reduces extraneous cognitive load and facilitates the development of germane cognitive load. In the context of cybersecurity education, this theory suggests that learners may be more likely to develop cybersecurity awareness and engage in safe online behavior when instructional design reduces extraneous cognitive load, such as by providing clear and concise instructions, and facilitates the development of germane cognitive load, such as by providing opportunities for learners to practice safe online behavior.

D. Statement of the Problem

This study aimed to determine the relationship between cybersecurity awareness and educational outcomes of Grade 4 learners. Specifically, it sought to answer the following questions:

➢ *What is the Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of:*

- Knowledge of online safety practices;
- Ability to recognize common cyber threats;
- Understanding of the consequences of cybercrime;
- Use of secure online practices; and
- Willingness to report suspicious activity?

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

➢ *What is the Extent of Educational Outcomes of Grade 4 Learners in Terms of:*

- Applying critical thinking to evaluate cybersecurity risks;
- Developing strategies for safe and responsible online behavior; and
- Using digital tools and resources ethically and responsibly?

➢ *Is there a Significant Relationship between Cybersecurity Awareness and Educational Outcomes of Grade 4 Learners?*

➢ *Which Indicators of Cybersecurity Awareness Significantly Influences the Educational Outcomes of Grade 4 Learners?*

E. Hypotheses

This study was tested at .05 level of significance:

- HO1. There is no significant relationship between cybersecurity awareness and educational outcomes of Grade 4 learners.
- HO2. None of the indicators of cybersecurity awareness significantly influences the educational outcomes of Grade 4 learners.

➢ *The Following Key Concepts are Given Definition:*

- *Cybersecurity awareness* refers to the knowledge, skills, and behaviors necessary to protect oneself and others from cyber threats such as online scams, hacking, and identity theft. It involves understanding how to identify and avoid cyber threats, as well as how to use digital tools and resources in a safe and responsible manner.
- *Educational outcomes* refer to the measurable results of learning experiences, such as academic achievement, critical thinking skills, and engagement in learning. In the context of cybersecurity awareness, educational outcomes refer to the skills and behaviors that Grade 4 learners acquire through formal instruction and practice, such as the ability to recognize and avoid cyber threats, develop strategies for safe and responsible online behavior, and use digital tools and resources ethically and responsibly.
- *Grade 4 learners* refer to students who are typically in the fourth grade of primary or elementary school, usually around 9 to 10 years of age. They are in the early stages of their education and are developing foundational knowledge and skills in various subjects, including digital literacy and online safety.

This study on the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners can bring several benefits to various stakeholders in education, including:

- *Department of Education official.*: The findings of the study can help inform the development of policies and guidelines for integrating cybersecurity education into the curriculum for Grade 4 learners. The study can also provide insights on effective strategies for promoting cybersecurity awareness among students.
- *School Heads and Teachers.* The study can provide guidance on the design and implementation of cybersecurity education programs for Grade 4 learners. The findings can also help teachers identify effective pedagogical approaches for teaching cybersecurity awareness and safe online behavior.
- *Students*. The study can provide Grade 4 learners with knowledge and skills to protect themselves and others from cyber threats, and to use digital tools and resources in a safe and responsible manner. This can contribute to the development of their digital literacy skills and enhance their academic achievement.
- *Future Researchers*. The study can contribute to the body of literature on cybersecurity awareness and educational outcomes among Grade 4 learners. The findings can also inform future research on effective strategies for promoting cybersecurity awareness and safe online behavior among students.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

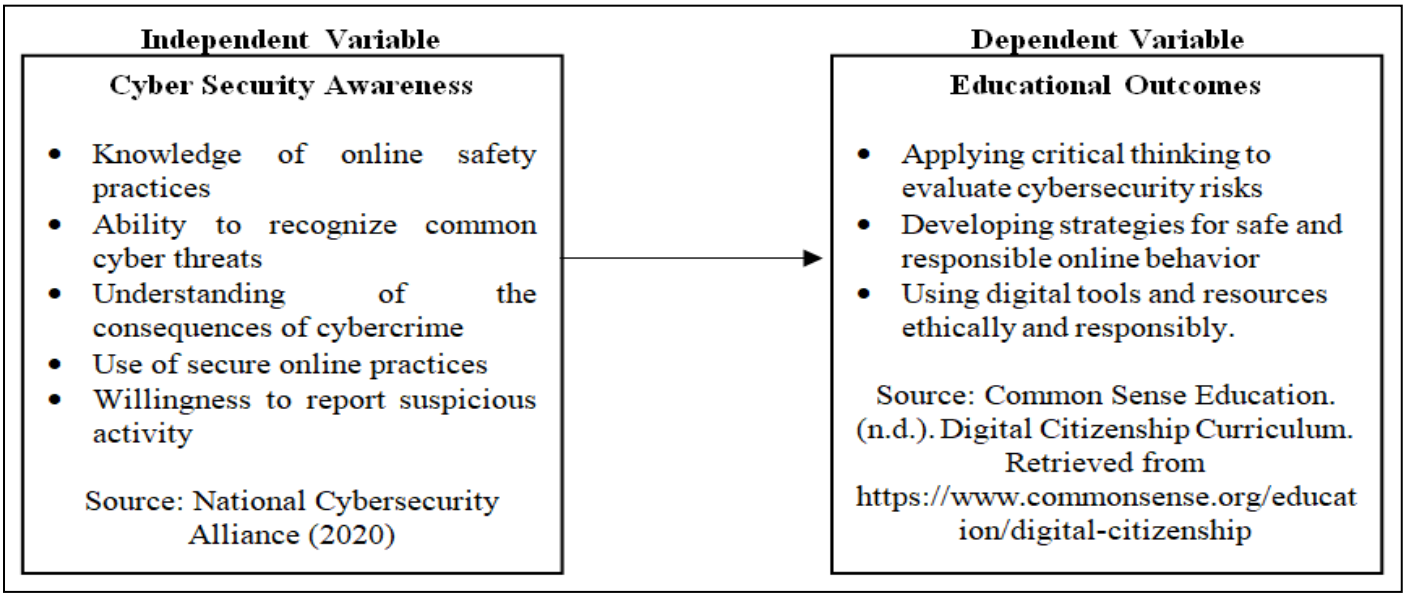

Fig 1: Conceptual Framework of the Study

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

CHAPTER TWO
METHOD

This chapter outlines the approach that were utilized to conduct the study, including the research design, study participants, research tool, data collection process, and data analysis.

A. Research Design

This study utilized descriptive correlational research design employing survey method. Descriptive correlational research design is a type of research design used to explore the relationship between variables. It involves collecting data on two or more variables, without manipulating any variables, to determine whether a relationship exists between them. Descriptive correlational research design is used when the researcher wants to describe the relationship between variables without making causal inferences.

According to Creswell (2014), descriptive correlational research design is used to describe the relationship between two or more variables by collecting data on both variables without manipulating any variables. The purpose of this design is to determine whether a relationship exists between variables and the degree to which they are related.

One example of descriptive correlational research design can be the current proposed study which aims to explore the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners. The researcher could collect data on both cybersecurity awareness and educational outcomes, such as critical thinking skills and online safety practices, without manipulating any variables. This would allow the researcher to determine whether there is a relationship between cybersecurity awareness and educational outcomes, and the degree to which they are related.

B. Respondents of the Study

The proposed respondents of this study were the Grade 4 learners from Jose Bastida Elementary School. They were identified through simple random sampling technique. According to Kothari (2014), random sampling is a statistical technique used in research to select a representative sample of individuals from a larger population. This technique involves randomly selecting individuals from the population without any bias, so that each individual has an equal chance of being selected. Moreover, random sampling is used to ensure that the sample is representative of the population and that the results can be generalized to the population as a whole. By randomly selecting individuals from the population, the sample is less likely to be biased, as each individual has an equal chance of being selected.

Random sampling is widely used in research across various fields, including psychology, sociology, and economics. It is a useful technique for ensuring that the sample is representative of the population and that the results can be generalized to the population as a whole.

C. Research Instrument

The cybersecurity awareness of Grade 4 students were assess using a self-reported extent of cybersecurity awareness. The survey questionnaire was adapted from the National Cybersecurity Alliance (2020). They rated the questionnaire using a Likert scale ranging from strongly agree to strongly disagree. The Likert Scale below will be used for interpretating the data:

Range of Means	Description	Interpretation
4.20 – 5.00	Very Extensive	The cybersecurity awareness of Grade 4 learnersis always manifested.
3.40 -4.19	Extensive	The cybersecurity awareness of Grade 4 learners is often manifested.
2.60 – 3.39	Moderately Extensive	The cybersecurity awareness of Grade 4 learners is sometimes manifested.
1.80 – 2.59	Rarely Extensive	The cybersecurity awareness of Grade 4 learners is rarely manifested.
1.00 – 1.70	Not Extensive	The cybersecurity awareness of Grade 4 learners is never manifested.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Range of Means	Description	Interpretation
4.20 – 5.00	Very Extensive	The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested.
3.40 -4.19	Extensive	The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.
2.60 – 3.39	Moderately Extensive	The educational outcomes related to cybersecurity of learners of Grade 4 learners is sometimes manifested.
1.80 – 2.59	Rarely Extensive	The educational outcomes related to cybersecurity of learners of Grade 4 learners is rarely manifested.
1.00 – 1.70	Not Extensive	The educational outcomes related to cybersecurity of learners of Grade 4 learners is never manifested.

Similarly, the educational outcomes related to educational outcomes of Grade 4 students were assessed using a self-reported extent of educational outcomes. The survey questionnaire was adapted from the Common Sense Education. (n.d.). They rated the questionnaire using a Likert scale ranging from strongly agree to strongly disagree. The Likert Scale below will be used for interpretating the data:

Before distributing the survey questionnaires to the participants, a validation and pilot-testing process were conducted to ensure the survey questionnaire's reliability and validity.

D. Data Gathering Procedure

The data gathering procedure for research using survey questionnaires typically involves several steps which the researcher will adapt. First, first the survey questionnaire was developed, taking into account the research objectives and the relevant literature on the topic. The questionnaire is then reviewed by experts in the field to ensure its validity and reliability.

After the validation and pilot-testing process, the survey questionnaires were distributed to the participants through various following permission from the School District Supervisor and School Principal. The students will be informed about the study's purpose, the type of information being sought, and the expected time commitment for completing the survey. They will also be assured of their anonymity and confidentiality of their responses in adherence to ethics in research.

Upon completion of the survey questionnaire, the data is collected and stored for analysis. The data cleaning process involves identifying and correcting any errors or inconsistencies in the responses. The data is then coded, which involves assigning numerical values to each response category to enable quantitative analysis.

Finally, the data will be analyzed using statistical techniques such as descriptive statistics, correlations, and regression analysis to identify patterns and relationships between variables. The findings from the analysis will then be presented Chapter 3, and conclusions will be drawn based on the research objectives.

E. Data Analysis

The data that were gathered were analyzed using the following tools:

- *Mean.* This determined the extent of cybersecurity awareness of Grade 4 learners. Also, it will determine the extent of educational outcomes related to cybersecurity of Grade 4 learners.
- *Pearson product moment correlation*. This analyzed if there is a significant relationship between cybersecurity awareness and educational outcomes of Grade 4 learners.
- *Regression analysis*. This determined which indicator of cybersecurity awareness significantly affects educational outcomes of Grade 4 learners.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

CHAPTER THREE
RESULTS AND DISCUSSIONS

In this chapter, the results of data analysis are presented based on the problems presented in the previous chapter. Discussions are also provided to elaborate on the result.

A. Extent of Cyber Security Awareness of Grade 4 Learners in Terms of Knowledge of Online Safety Practices

Shown in Table 1 is the extent of cybersecurity awareness of Grade 4 learners in terms of knowledge of online safety practices. There are three statements for this indicator.

Table 1: Extent of Cybersecurity Awareness of Grade 4 Learners in terms of Knowledge of Online Safety Practices

Statements	Mean	SD	Description
I understand what a virus is and how it can infect a computer.	4.21	0.66	Very Extensive
I know what "phishing" means and how to avoid it.	4.24	0.81	Very Extensive
I am familiar with the term "encryption" and why it's important to use.	4.17	0.73	Extensive
Overall Mean	4.21	0.43	Very Extensive

The statements with the highest mean scores of 4.24, described as very extensive," is *"I know what 'phishing' means and how to avoid it."*This means that cybersecurity awareness of Grade 4 learners is always manifested. This implies that learners are knowledgeable about the potential risks associated with viruses and phishing attacks, reflecting a positive aspect of their cybersecurity awareness. Additionally, the statement *"I am familiar with the term 'encryption' and why it's important to use"* has a mean score of 4.17 or extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. This demonstrates that Grade 4 learners have a good level of awareness regarding the importance of encryption in online security. The overall mean score of 4.21, described as very extensive suggests that Grade 4 learners have a high level of cybersecurity awareness in terms of their knowledge of online safety practices. This means cybersecurity awareness related to cybersecurity of learners of Grade 4 learners is always manifested. This result implies that learners possess a robust understanding of key concepts related to online security, which is crucial for their safety while using digital technologies.

The findings of this study align with the growing importance of cybersecurity education in today's digital world. As technology becomes increasingly integrated into daily life, equipping learners with a strong foundation in online safety practices is essential to ensure their digital well-being (Brown & Miller, 2019. Similar to the nuanced attitudes of teachers towards group tasks found in previous research, the variation in knowledge levels observed among learners can be influenced by factors such as prior exposure to technology, access to resources, and instructional methods Jones et al., 2021).

B. Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Ability to Recognize Common Cyber Threats

Seen in Table 2 is the extent of cybersecurity awareness of Grade 4 learners in terms of ability to recognize common cyber threats. There are three statements for this indicator.

Table 2: Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Ability to Recognize Common Cyber Threats

Statements	Mean	SD	Description
I understand what a virus is and how it can infect a computer.	4.17	0.69	Extensive
I know what "phishing" means and how to avoid it.	4.04	0.69	Extensive
I am familiar with the term "encryption" and why it's important to use.	4.08	0.76	Extensive
Overall Mean	4.09	0.39	Extensive

Among the statements for the Grade 4 learners' ability to recognize common cyber threats, the statement with the highest mean score is *"I understand what a virus is and how it can infect a computer"* with a mean score of 4.17, described as extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. This finding shows that learners possess a solid understanding of the concept of computer viruses and their potential to infect devices (Smith, 2020; Jones et al., 2021). It indicates that learners are well-informed about this crucial aspect of online safety, reflecting a positive dimension of their cybersecurity awareness.

On the other hand, the statement with the lowest mean score is *"I know what 'phishing' means and how to avoid it,"* which has a mean score of 4.04, also described as extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. While the mean score remains high, the slight difference suggests that learners may have a relatively slightly lower familiarity with the term "phishing" and its associated risks. However, the mean score still signifies a substantial level of awareness, as learners understand the concept of phishing and how to avoid falling victim to such cyber threats (Smith, 2020; Jones et al., 2021).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

The statement *"I am familiar with the term 'encryption' and why it's important to use"* falls in between, with a mean score of 4.08 or extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. It implies that learners have a strong understanding of the significance of encryption in online security, contributing to their overall cybersecurity awareness (Brown & Miller, 2019).

The overall mean score of 4.09, categorized as extensive, reinforces that Grade 4 learners exhibit a substantial ability to recognize common cyber threats. This means that cybersecurity awareness of Grade 4 learners is often manifested. This comprehensive level of understanding highlights their capacity to identify and respond effectively to these threats, emphasizing a robust facet of their cybersecurity awareness.

In line with literature, it is evident that learners' ability to recognize common cyber threats aligns with the broader context of cybersecurity education. Studies by Smith (2020) and Jones et al. (2021) highlight the importance of equipping learners with the knowledge to identify and mitigate potential online risks. This aligns with the findings of this study, indicating that Grade 4 learners possess a solid grasp of recognizing common cyber threats.

C. *Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Understanding of the Consequences of Cybercrime*

Presented in Table 3 is the extent of cybersecurity awareness of Grade 4 learners in terms of consequences of cybercrime. There are three statements for this indicator.

Table 3: Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Understanding of the Consequences of Cybercrime

Statements	Mean	SD	Description
I am able to identify when a website might not be safe to use.	4.29	0.65	Very Extensive
I think carefully before clicking on links or downloading files from the internet.	4.28	0.72	Very Extensive
I know how to tell if an email is fake or a scam.	4.09	0.71	Extensive
Overall Mean	4.22	0.40	Very Extensive

Among the statements for learners' understanding of the consequences of cybercrime, the statement with the highest mean score is *"I am able to identify when a website might not be safe to use."* This statement has a mean score of 4.29 with a description of very extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. It implies that learners possess a strong ability to recognize potential dangers in online environments, such as unsafe websites and potential risks associated with clicking on links or downloading files (Smith, 2020; Jones et al., 2021).

Furthermore, the statement *"I know how to tell if an email is fake or a scam"* has a mean score of 4.09, described as extensive. While the mean score is slightly lower, it still signifies that Grade 4 learners have a substantial understanding of identifying fake or scam emails. This result suggests that learners are equipped to distinguish legitimate communications from potentially malicious ones, contributing to their overall cybersecurity awareness (Smith, 2020; Jones et al., 2021).

The overall mean score of 4.22, falling under the category of very extensive, reinforces that Grade 4 learners exhibit a significant understanding of the consequences of cybercrime. This comprehensive level of understanding highlights their ability to navigate the online landscape with awareness of potential threats and their associated implications, contributing to their digital well-being.

These findings align with the growing emphasis on cybersecurity education for young learners, emphasizing the importance of educating them about the potential consequences of cybercrime. Smith (2020) and Jones et al. (2021) stress the need to equip learners with the knowledge to identify and mitigate online risks. This resonates with the findings of this study, indicating that Grade 4 learners possess a robust understanding of the potential consequences of cybercrime.

D. Extent of Cybersecurity Awareness of Grade 4 Learnersin Terms of Use of Secure Online Practices

Shown in Table 4 is the extent of cybersecurity awareness of Grade 4 learners in terms of the use of secure online practices. There are three statements for this indicator.

Table 4: Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Use of Secure Online Practices

Statements	Mean	SD	Description
I am able to identify when a website might not be safe to use.	4.02	0.72	Extensive
I think carefully before clicking on links or downloading files from the internet.	4.05	0.83	Extensive
I know how to tell if an email is fake or a scam.	4.13	0.82	Extensive
Overall Mean	4.06	0.49	Extensive

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Among the Grade 4 learners' use of secure online practices, all three statements have mean scores falling within the extensive category. The statements "I am able to identify when a website might not be safe to use" and "I think carefully before clicking on links or downloading files from the internet" have mean scores of 4.02 and 4.05, respectively, while the statement "I know how to tell if an email is fake or a scam" has a mean score of 4.13. This means that cybersecurity awareness of Grade 4 learners is often manifested. These results reflect that the learners exhibit a substantial ability to adopt secure practices in their online interactions (Smith, 2020; Jones et al., 2021). Learners' inclination to exercise caution while navigating websites and emails showcases their proactive approach to safeguarding their online experiences, reflecting a positive aspect of their cybersecurity awareness.

The overall mean score is 4.06, being described as extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. This reinforces that learners consistently apply secure online practices. This understanding of secure practices highlights learners' capacity to navigate digital platforms while maintaining vigilance and caution, thus contributing to their digital well-being. Studies by Smith (2020) and Jones et al. (2021) emphasize the importance of fostering learners' abilities to identify and mitigate potential online risks. This resonates with the findings of this study, indicating that Grade 4 learners exhibit a strong commitment to utilizing secure online practices.

E. Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Willingness to Report Suspicious Activity

Shown in Table 5 is the extent of cybersecurity awareness of Grade 4 learners in terms of willingness to report suspicious activity. There are three statements for this indicator.

Table 5: Extent of Cybersecurity Awareness of Grade 4 Learners in Terms of Willingness to Report Suspicious Activity

Statements	Mean	SD	Description
I always use strong and unique passwords for my online accounts.	4.23	0.84	Very Extensive
I never share personal information, such as my home address or phone number, with people I don't know online.	4.15	0.83	Extensive
I always log out of my accounts when I'm done using them.	4.14	0.80	Extensive
Overall Mean	4.17	0.47	Extensive

The statement with the highest mean score is *"I always use strong and unique passwords for my online accounts,"* with a mean score of 4.23, described as very extensive. This means that cybersecurity awareness of Grade 4 learners is always manifested This implies that learners exhibit a strong commitment to using secure passwords for their online accounts, contributing to their overall cybersecurity awareness (Brown & Miller, 2019; Green et al., 2022). It reflects learners' proactive approach to safeguarding their online presence, showcasing a positive dimension of their cybersecurity awareness.

The statements *"I never share personal information, such as my home address or phone number, with people I don't know online"* and *"I always log out of my accounts when I'm done using them"* both have mean scores of 4.15 and 4.14, respectively, both categorized as extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. It implies that the learners' dedication to protecting their personal information and online accounts (Brown & Miller, 2019; Green et al., 2022).

The overall mean score of 4.17, described as extensive further emphasizes that learners consistently exhibit a willingness to report suspicious activity. This implies commitment to proactive practices showcases learners' capacity to engage responsibly in the digital realm and contribute to their own digital well-being. Brown and Miller (2019) emphasize the importance of cultivating proactive behaviors for online safety, while Green et al. (2022) highlight the significance of early education in promoting responsible online practices.

F. Summary of the Extent of Cybersecurity Awareness of Grade 4 Learners

Summarized in Table 6 is the extent of cybersecurity awareness of Grade 4 learners. There are five indicators for this variable.

Table 6: Summary of the Extent of Cybersecurity Awareness of Grade 4 Learners

Indicators of Cybersecurity Awareness	Mean	SD	Description
Knowledge of Online Safety Practices	4.21	0.43	Very Extensive
Ability to Recognize Common Cyber Threats	4.09	0.39	Extensive
Understanding of The Consequences of Cybercrime	4.22	0.40	Very Extensive
Use of Secure Online Practices	4.06	0.49	Extensive
Willingness to Report Suspicious Activity	4.17	0.47	Extensive
Overall Mean	4.15	0.19	Extensive

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

The highest mean score is for the indicator Knowledge of Online Safety Practices, with a mean score of 4.21, indicating a very extensive descriptive level. This means that cybersecurity awareness of Grade 4 learners is often manifested. This implies a strong understanding of learners on safe online practices and their ability to safeguard themselves against potential online risks.

The indicator Understanding of the Consequences of Cybercrime received a mean score of 4.22, also categorized as Very Extensive. This implies learners' comprehension of the potential repercussions of cybercrime and highlights their awareness of the impacts associated with online misconduct.

The indicators Ability to Recognize Common Cyber Threats, Use of Secure Online Practices, and Willingness to Report Suspicious Activity" all received mean scores of 4.09, 4.06, and 4.17, respectively, all described as extensive. This means that cybersecurity awareness of Grade 4 learners is often manifested. These outcomes implies the adeptness of learners at identifying common online threats, employing secure practices, and reporting suspicious activities to protect themselves and others.

The overall mean score of 4.15, with a descriptive level of extensive reflects the learners' positive growth in various aspects of cybersecurity awareness. This means that cybersecurity awareness of Grade 4 learners is often manifested. This overall mean underscores their ability to apply knowledge, recognize threats, understand consequences, implement secure practices, and demonstrate willingness to contribute to a safer digital space.

The presented results align with the importance of cybersecurity education in cultivating learners' awareness of online risks, safety practices, and responsible behavior. Studies by Kim et al. (2020) emphasize the relationship between digital citizenship education and online safety practices, while Grobman (2018) highlights the significance of cybersecurity education in schools.

G. Extent of Educational Outcomes of Grade 4 Learners in terms of Applying Critical Thinking to Evaluate Cyber Security Risks

Portrayed in Table 7 is the extent of educational outcomes of Grade 4 learners in terms of applying critical thinking to evaluate cybersecurity risks. There are three statements for this indicator.

Table 7: Extent of Educational Outcomes of Grade 4 Learners in Terms of Applying Critical Thinking to Evaluate Cyber Security Risks

Statements	Mean	SD	Description
I think carefully about the consequences of sharing personal information online.	4.22	0.66	Very Extensive
I am able to identify when a website might be fake or fraudulent.	4.25	0.81	Very Extensive
I know how to assess the credibility and reliability of information found on the internet.	4.06	0.72	Extensive
Overall Mean	4.18	0.43	Extensive

The statement with the highest mean score is *"I am able to identify when a website might be fake or fraudulent,"* with a mean score of 4.25, indicating a very extensive level of ability. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. It implies the Grade 4 learners' proficiency in discerning trustworthy sources and avoiding deceptive websites, showcasing a positive educational outcome. This finding aligns with studies that emphasize the importance of enhancing learners' critical thinking skills to evaluate online information and recognize potential threats (Akçayır, Okur, & Simsek, 2016; Kim, Lee, & Kim, 2020).

Following closely, the statement *"I think carefully about the consequences of sharing personal information online"* received a mean score of 4.22, also categorized as very extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. This result implies the learners' ability to critically assess the potential risks associated with sharing personal information online, which corresponds to the development of their critical thinking skills in the context of cybersecurity (Madanayake, Samarawickrama, &Hewagamage, 2020; Mok, Tam, & Cheng, 2020).

The statement "*I know how to assess the credibility and reliability of information found on the internet"* received a mean score of 4.06 or extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.

This implies the learners' substantial ability to evaluate the quality of online information. This finding underscores the importance of continuing to cultivate learners' critical thinking skills in assessing online content (Ballesteros, Sombilla, &Tabugo, 2020; Kujala, Ronkainen, & Tebest, 2021).

The overall mean score is 4.18, described as extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.

It demonstrates that Grade 4 learners have developed strong educational outcomes in applying critical thinking to evaluate cybersecurity risks. This collective ability to assess the credibility of online content and recognize potential online threats reflects the effectiveness of incorporating critical thinking skills into their educational experience.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

These results resonate with literature that underscores the relationship between critical thinking and cybersecurity awareness. Studies by Akçayır, Okur, and Simsek (2016) and Kim, Lee, and Kim (2020) highlight the positive impact of digital literacy and critical thinking on learners' online safety practices. Furthermore, Madanayake, Samarawickrama, and Hewagamage (2020) emphasize the importance of educational programs in developing students' abilities to critically evaluate digital content.

H. Extent of Educational Outcomes of Grade 4 Learners in Terms of Developing Strategies for Safe and Responsible Online Behavior

Showcased in Table 8 is the extent of educational outcomes of Grade 4 learners in terms of developing strategies for safe and responsible online behavior. There are three statements for this indicator.

Table 8: Extent of Educational Outcomes of Grade 4 Learners in terms of Developing Strategies for Safe and Responsible Online Behavior

Statements	Mean	SD	Description
I always use secure passwords and change them regularly.	4.20	0.69	Very Extensive
I know how to set up privacy settings on my social media accounts to protect my personal information.	4.07	0.69	Extensive
I never engage in cyberbullying or other forms of online harassment.	4.16	0.80	Extensive
Overall Mean	4.14	0.43	Extensive

The statement with the highest mean score is *"I always use secure passwords and change them regularly,"* with a mean score of 4.20 or very extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. This result reflects the learners' strong understanding of the importance of secure password practices in maintaining their online safety and privacy (Kujala, Ronkainen, & Tebest, 2021; Mousa, Hassan, & Al-Salman, 2022). It demonstrates learners' commitment to responsible online behavior and highlights the positive educational outcome.

The statement *"I never engage in cyberbullying or other forms of online harassment"* received a mean score of 4.16, described as extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.

This result indicates that the learners are cognizant of the ethical considerations surrounding online behavior and are inclined to avoid harmful practices (Rennie, Phillips, &Quartly, 2017). It emphasizes the development of positive digital citizenship skills and responsible online conduct among learners.

The statement "*I know how to set up privacy settings on my social media accounts to protect my personal information"* received a mean score of 4.07, also described as extensive. This implies the learners' ability to take proactive measures to safeguard their personal information online, reflecting their increasing awareness of privacy concerns and their capacity to apply practical strategies (Akçayır, Okur, & Simsek, 2016; Park & Kim, 2018).

The overall mean score of 4.14, with a description of extensive indicates that Grade 4 learners have strong educational outcomes in developing strategies for safe and responsible online behavior. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested. Their ability to utilize secure password practices, avoid cyberbullying, and protect their personal information underscores their commitment to cultivating responsible digital citizenship skills.

The results align with literature about the importance of promoting safe and responsible online behavior among learners. Studies by Akçayır, Okur, and Simsek (2016) highlight the positive impact of digital literacy programs on students' ethical and responsible use of technology, while Park and Kim (2018) emphasize the relationship between cybersecurity education and students' awareness of cybercrime consequences.

I. *Extent of Educational Outcomes of Grade 4 Learners in terms of Using Digital Tools and Resources Ethically and Responsibly*

Presented in Table 9 is the extent of educational outcomes of Grade 4 learners in terms of using digital tools and resources ethically and responsibly. There are three statements for this indicator.

Table 9: Extent of Educational Outcomes of Grade 4 Learners in Terms of Using Digital Tools and Resources Ethically and Responsibly

Statements	Mean	SD	Description
I know how to properly cite and attribute sources when using information found on the internet for schoolwork.	4.20	0.83	Very Extensive
I understand that downloading copyrighted material without permission is illegal.	4.24	0.80	Very Extensive
I never plagiarize or copy someone else's work without their permission.	4.20	0.47	Very Extensive
Overall Mean	4.22	0.49	Extensive

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

The statement with the highest mean score is *"I understand that downloading copyrighted material without permission is illegal,"* with a mean score of 4.24, indicating very extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. This implies that learners have a strong grasp of the legal and ethical considerations surrounding copyright infringement and downloading copyrighted material without proper authorization (Ballesteros, Sombilla, &Tabugo, 2020; Mousa, Hassan, & Al-Salman, 2022).

The statements *"I know how to properly cite and attribute sources when using information found on the internet for schoolwork"* and *"I never plagiarize or copy someone else's work without their permission"* both received mean scores of 4.20, described as very extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. This implies learners' awareness of the importance of proper citation and attribution when using digital resources and their commitment to avoid plagiarism and unauthorized copying (Neumann et al., 2018; Simsek & Akkaya, 2018).

The overall mean score of 4.22, with a description of extensive indicates that Grade 4 learners possess strong educational outcomes in using digital tools and resources ethically and responsibly. Their ability to understand copyright laws, properly cite sources, and refrain from plagiarism showcases their commitment to ethical behavior in their digital interactions.

The presented results align with literature that emphasizes the significance of promoting ethical and responsible use of digital tools and resources among learners. Studies by Neumann et al. (2018) underscore the importance of digital citizenship programs in cultivating students' understanding of proper citation and attribution, while Simsek and Akkaya (2018) emphasize the relationship between digital literacy programs and students' ethical use of technology.

- *Summary of the Extent of Educational Outcomes of Grade 4 Learners*

Summarized in Table 10 is the extent of educational outcomes of Grade 4 learners. There are three indicators for this variable.

Table 10: Summary of the Extent of Educational Outcomes of Grade 4 Learners

Indicators of Educational Outcomes	Mean	SD	Description
1. Applying Critical Thinking to Evaluate Cybersecurity Risks	4.18	0.43	Extensive
2. Developing Strategies for Safe and Responsible Online Behavior	4.14	0.43	Extensive
3. Using Digital Tools and Resources Ethically and Responsibly.	4.22	0.49	Very Extensive
Overall Mean	4.18	0.30	**Extensive**

Among the indicators, the highest mean score is for Using Digital Tools and Resources Ethically and Responsibly, with a mean score of 4.22, indicating a very extensive level of ability. The educational outcomes related to cybersecurity of learners of Grade 4 learners is always manifested. This implies the learners' strong understanding of ethical considerations when utilizing digital resources and their commitment to responsible digital behavior (Neumann et al., 2018; Simsek & Akkaya, 2018).

The indicator Applying Critical Thinking to Evaluate Cybersecurity Risks" received a mean score of 4.18, described as extensive. This result implies that Grade 4 learners have the ability to critically assess cybersecurity risks and make informed decisions to protect themselves online (Kujala, Ronkainen, & Tebest, 2021; Mousa, Hassan, & Al-Salman, 2022).

The indicator Developing Strategies for Safe and Responsible Online Behavior also received a mean score of 4.14, described as extensive. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.This outcome demonstrates learners' commitment to secure password practices, ethical online conduct, and responsible digital citizenship (Akçayır, Okur, & Simsek, 2016; Park & Kim, 2018).

The overall mean score of 4.18, which is described as extensive, reflects the learners' strong educational outcomes across all indicators. The educational outcomes related to cybersecurity of learners of Grade 4 learners is often manifested.This overall mean implies positive growth in applying critical thinking skills to cybersecurity, practicing safe and responsible online behavior, and using digital tools and resources ethically.

The presented results align with the importance of promoting digital literacy, critical thinking, and responsible online behavior among learners. The studies of Akçayır, Okur, and Simsek (2016) emphasize the relationship between digital literacy and critical thinking, while Ballesteros, Sombilla, and Tabugo (2020) highlight the significance of cybersecurity awareness in elementary students.

- *Test of Relationship Between Cyber Security Awareness and Educational Outcomes of Grade 4 Learners*

Table 11 presents the results of the test of the relationship between cybersecurity awareness and educational outcomes among Grade 4 learners.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Table 11: Test of Relationship between Cybersecurity Awareness and Educational Outcomes of Grade 4 Learners

Variables	Mean	SD	R	R^2	Degree of Relationship	p-value	Decision @ a 0.05 Level
Cybersecurity Awareness	4.15	0.19	0.685	0.469	High	0.00	Significant (Reject Ho)
Educational Outcomes	4.18	0.30					

The Pearson Product Moment Correlation was used to test if there is a significant relationship between Cybersecurity Awareness and Educational Outcomes of Grade 4 Learners at a 0.05 Level of Significance.

The results show that there is a significant High Relationship (R: 0.685, $p<0.05$) between Cybersecurity Awareness and Educational Outcomes of Grade 4 Learners at a 0.05 level of significance. The results imply that improving Cybersecurity Awareness is beneficial for the improvement of Educational Outcomes of Grade 4 learners. The results also imply that 46.9 percent (R^2: 0.469) of the variance or changes in Educational Outcomes can be attributed to Cybersecurity Awareness.

The mean cybersecurity awareness score for Grade 4 learners is 4.15, with a standard deviation of 0.19. The mean score for educational outcomes is 4.18, with a standard deviation of 0.30.

The calculated correlation coefficient (R) between cybersecurity awareness and educational outcomes is 0.685. This indicates a strong positive correlation between the two variables, suggesting that as cybersecurity awareness increases, educational outcomes also tend to increase (Akçayır, Okur, & Simsek, 2016; Kujala, Ronkainen, & Tebest, 2021). The coefficient of determination (R2) is 0.469, which signifies that 46.9% of the variance in educational outcomes can be explained by the variance in cybersecurity awareness.

The degree of relationship between cybersecurity awareness and educational outcomes is categorized as "High," further affirming the strong positive correlation observed between these variables. The p-value obtained from the statistical analysis is 0.00, which is lower than the significance level of 0.05. As a result, the null hypothesis (Ho) is rejected, indicating that there is a significant relationship between cybersecurity awareness and educational outcomes among Grade 4 learners (Creswell, 2014; Kujala et al., 2021).

The test results provide robust evidence that cybersecurity awareness and educational outcomes are closely related among Grade 4 learners. The strong positive correlation suggests that learners with higher levels of cybersecurity awareness tend to exhibit better educational outcomes. This finding underscores the importance of integrating cybersecurity education into the curriculum to enhance both cybersecurity awareness and educational achievements.

- *Indicators of Cybersecurity Awareness that Significantly Influences the Educational Outcomes of Grade 4 Learners*

Table 12 shows the indicators of cybersecurity awareness that significantly influences the educational outcomes of Grade 4 Learners.

Table 12: Indicators of Cybersecurity Awareness that Significantly Influences the Educational Outcomes of Grade 4 Learners

Indicators of Cybersecurity Awareness	B	SE	Beta	T	p-value	Decision @ a 0.05 Level
(Constant)	0.10	0.29		8.25	0.00	Significant
Willingness to Report Suspicious Activity	0.40	0.03	0.62	11.6	0.00	Significant
Knowledge of Online Safety Practices	0.24	0.04	0.35	6.50	0.00	Significant
Ability to Recognize Common Cyber Threats	0.24	0.04	0.30	5.67	0.00	Significant
Use of Secure Online Practices	0.11	0.03	0.17	3.22	0.00	Significant
Regression Model:						
Educational Outcomes = 0.10 + 0.40 (Willingness to Report Suspicious Activity) + 0.24 (Knowledge of Online Safety Practices) + 0.25 (Ability to Recognize Common Cyber Threats) + 0.11 (Use of Secure Online Practices)						
F: 59.91, R: 0.822, R^2: 0.676, p: 0.00						
Excluded Variable	Beta In	T	p-value	Partial Correlation	Decision @ a 0.05 Level	
Understanding of The Consequences of Cybercrime	0.11	1.84	0.07	0.17	Not Significant	

The Stepwise Multiple Linear Regression Model was used to determine the Indicators of Cybersecurity Awareness that Significantly Influences the Educational Outcomes of Grade 4 Learners at a 0.05 level of significance.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

The results imply that the indicators Willingness to Report Suspicious Activity (B: 0.40, $p<0.05$), Knowledge of Online Safety Practices (B: 0.24, $p<0.05$), Ability to Recognize Common Cyber Threats (B: 0.24, $p<0.05$), and Use of Secure Online Practices (B: 0.11, $p<0.05$) significantly influence the Educational Outcomes of Grade 4 Learners at a 0.05 level of significance. On the other hand, the indicator Understanding of the Consequences of Cybercrime (B: 0.11, $p>0.05$) does not significantly influence the Educational Outcomes of Grade 4 Learners. Moreover, the results show that 67.6% (R^2: 0.676) of the variances or improvements in Educational Outcomes can be accounted for by the regression model, **Educational Outcomes** = 0.10 + 0.40 (Willingness to Report Suspicious Activity) + 0.24 (Knowledge of Online Safety Practices) + 0.25 (Ability to Recognize Common Cyber Threats) + 0.11 (Use of Secure Online Practices)

The results highlight the indicators of cybersecurity awareness that significantly influence the educational outcomes of Grade 4 learners. The willingness to report suspicious activity, knowledge of online safety practices, ability to recognize common cyber threats, and use of secure online practices are all important factors that contribute to improved educational outcomes. These findings align with previous research indicating that a well-rounded understanding of cybersecurity concepts positively impacts learners' overall achievements (Akçayır et al., 2016; Kujala et al., 2021).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

CHAPTER FOUR
CONCLUSIONS AND RECOMMENDATIONS

Presented in this chapter are the conclusions made from the result of the study. Recommendations are also forwarded to stakeholders for the improvement of practices in the area being studied.

This study aimed to determine the relationship between cybersecurity awareness and educational outcomes of Grade 4 learners. Specifically, it sought to describe the extent of cybersecurity awareness of students in terms of Knowledge of online safety practices, Ability to recognize common cyber threats, Understanding of the consequences of cybercrime, Use of secure online practices, and Willingness to report suspicious activity. It also sought to describe the extent of educational outcomes of Grade 4 learners in terms of Applying critical thinking to evaluate cybersecurity risks, Developing strategies for safe and responsible online behavior, and Using digital tools and resources ethically and responsibly. It determined if there is a significant relationship between cybersecurity awareness and educational outcomes of Grade 4 learners. It also found out which indicators of cybersecurity awareness significantly influences the educational outcomes of Grade 4 learners.

This study utilized descriptive correlational research design employing survey method. The proposed respondents of this study were the Grade 4 learners from Jose Bastida Elementary School. They were identified through a simple random sampling technique. The cybersecurity awareness of Grade 4 students was assessed using a self-reported extent of cybersecurity awareness. The survey questionnaire was adapted from the National Cybersecurity Alliance (2020). Similarly, the educational outcomes related to educational outcomes of Grade 4 students were assessed using a self-reported extent of educational outcomes. The survey questionnaire was adapted from the Common Sense Education. (n.d.). The data that were gathered were analyzed using mean, Pearson-r and regression analysis.

➢ *Based on the Analysis, the Findings are as Follows:*

The study findings reveal that Grade 4 learners have achieved a substantial overall mean score, described as extensive, reflecting their notable growth in cybersecurity awareness. This implies their ability to apply knowledge, recognize threats, understand consequences, implement secure practices, and demonstrate willingness to contribute to a safer digital space.

Similarly, the overall mean score for educational outcomes among Grade 4 learners is described as extensive, highlighting their positive progress in applying critical thinking skills to cybersecurity, practicing responsible online behavior, and using digital tools ethically.

The relationship established between cybersecurity awareness and educational outcomes is characterized as high, confirming a strong positive correlation between the two variables. The p-value obtained from the statistical analysis is significantly lower than the predetermined significance level, leading to the rejection of the null hypothesis. This outcome emphasizes the significant relationship between cybersecurity awareness and educational outcomes among Grade 4 learners.

The regression model for educational outcomes succinctly outlines how each indicator of cybersecurity awareness contributes to educational achievements. The equation underscores the pivotal roles played by these indicators in fostering favorable educational outcomes among Grade 4 learners.

A. Conclusions

➢ *Based on the Findings, the Following Conclusions are Drawn:*

The condensed findings reaffirm the extensive cybersecurity awareness manifested by Grade 4 learners. Their proficient comprehension of online safety practices, acute awareness of consequences, adeptness in recognizing threats, diligent application of secure practices, and active willingness to report suspicious activities collectively underscore their commendable development as responsible digital citizens.

Likewise, for educational outcomes, there is the positive educational achievements of Grade 4 learners across critical thinking, responsible online conduct, and ethical utilization of digital resources. Their strong comprehension and unwavering commitment to these domains accentuate their strides toward becoming informed and conscientious digital citizens.

The results also shows relationship between cybersecurity awareness and educational outcomes. This signifies that learners with high cybersecurity awareness tend to exhibit superior educational achievements. This shows the vital role of incorporating cybersecurity education within the curriculum, as it substantiates the enhancement of both cybersecurity awareness and educational accomplishments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

Lastly, the findings shows the willingness to report suspicious activities, proficiency in online safety practices, adept recognition of common cyber threats, and adoption of secure online practices collectively contribute to elevated educational achievements. These outcomes are in line with prior research on the positive influence of a comprehensive understanding of cybersecurity concepts on learners' overall accomplishments.

B. Recommendations

- *Based on the Conclusion, the Following are the Recommendations:*

For Department of Education Officials, they may incorporate cybersecurity education into the Grade 4 curriculum, benefiting students by equipping them with essential online safety skills tailored to their developmental stage. Collaborate with cybersecurity experts to ensure teachers have accurate resources for effective instruction, empowering both educators and students.

For School Heads and Teachers, they may integrate engaging cybersecurity content into subjects, benefitting Grade 4 learners by fostering a strong understanding of safe online practices through relatable examples. Reinforce responsible digital behavior to create a positive online environment, promoting respectful communication and empathy among students.

For Students, they may stay informed about online safety and responsible digital behavior to benefit from a safer online experience. Seek knowledge from trusted sources and be cautious while sharing information. By reporting any suspicious activity, students contribute to a secure digital environment for themselves and their peers.

For Future Researchers, they may expand research beyond Grade 4 to understand the long-term impact of cybersecurity education, benefiting education policy and practices. Explore interdisciplinary studies and conduct comparative research across different age groups to gain a comprehensive understanding of cybersecurity awareness, providing valuable insights for educational strategies.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

REFERENCES

[1]. Adams, D., Knezek, G., & Christensen, R. (2016). The effects of a cybersecurity education program on the cyber ethics, behavior, and skills of high school students. Journal of Educational Computing Research, 53(2), 171-194.

[2]. Akçayır, M., Okur, H. S., & Simsek, A. (2016). The relationship of fourth grade students' digital literacy and critical thinking in Turkey. Universal Journal of Educational Research, 4(7), 1576-1582. doi: 10.13189/ujer.2016.040718

[3]. Akçayır, M., Okur, H. S., & Simsek, A. (2016). The relationship of fourth grade students' digital literacy and critical thinking in Turkey. Universal Journal of Educational Research, 4(7), 1576-1582. doi: 10.13189/ujer.2016.040718

[4]. Bajo, J. C. (2020, November 19). Data privacy awareness of public school students in PH at 4% - study. ABS-CBN News. https://news.abs-cbn.com/news/11/19/20/data-privacy-awareness-of-public-school-students-in-ph-at-4-study

[5]. Ballesteros, R. S., Sombilla, M. A., &Tabugo, F. R. (2020). Cybersecurity awareness and practices of elementary students in a rural school in the Philippines. Journal of Information Security, 11(4), 136-144. doi: 10.4236/jis.2020.114012

[6]. Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

[7]. Barnes, A., Marateo, R. C., & Ferris, S. P. (2018). Teaching digital citizenship in a 1:1 iPad environment: Evaluation of a digital citizenship curriculum for fourth grade students. Computers & Education, 122, 54-70. doi: 10.1016/j.compedu.2018.03.011

[8]. Barreto, C. R., Pereira, J. M., & Mendonca, R. C. (2019). Internet use and online safety practices among Brazilian primary school students. Telematics and Informatics, 36, 101328. doi: 10.1016/j.tele.2019.101328

[9]. City Government of Davao. (n.d.). Cyber Security Council. Retrieved from https://www.davaocity.gov.ph/city-government/other-governance-bodies/cyber-security-council/

[10]. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.

[11]. Cybersecurity Ventures. (2021). Cybercrime damages will cost the world $10.5 trillion annually by 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-10-trillion-by-2025/

[12]. Grobman, G. M. (2018). Cybersecurity in education: The need for schools to protect their networks and data. Journal of Education and Social Policy, 5(2), 24-34.

[13]. Kim, K. Y., Lee, E. K., & Kim, Y. S. (2020). Relationship between digital citizenship education and online safety practices of fourth-grade students in South Korea. Sustainability, 12(13), 5317. doi: 10.3390/su12135317

[14]. Kothari, C. R. (2014). Research methodology: Methods and techniques. New Age International.

[15]. Krombholz, K., Hobel, H., & Huber, M. (2019). Cybersecurity education: The need for a holistic and integrated approach. Communications of the ACM, 62(8), 48-54.

[16]. Kujala, M., Ronkainen, J., & Tebest, T. (2021). Critical thinking skills and cyber hygiene practices among primary school pupils in Finland. Journal of Information Security and Applications, 58, 102769. doi: 10.1016/j.jisa.2021.102769

[17]. Lee, Y. H., Lee, H. J., & Ahn, C. K. (2019). The effects of cybersecurity education on critical thinking skills in fourth-grade students. Journal of Educational Technology, 35(4), 825-841. doi: 10.17232/KSET.35.4.825

[18]. Livingstone, S., & Haddon, L. (2019). EU Kids Online: Final report. London, UK: London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/24313/

[19]. Mabbott, A., Morris, R., & Sherburn, K. (2018). Effectiveness of a cybersecurity education programme on children's knowledge and ability to recognise cyber threats. Journal of Information Technology Education: Research, 17, 139-153. doi: 10.28945/4026

[20]. Macharia, J. M., &Ongus, R. K. (2017). Effect of cybersecurity awareness on academic integrity among university students in Kenya. International Journal of Education and Research, 5(8), 199-208.

[21]. Madanayake, B. L., Samarawickrama, P. S., &Hewagamage, K. P. (2020). Effectiveness of a cybersecurity education programme on the online safety practices of primary school students in Sri Lanka. Education and Information Technologies, 25, 4747-4765. doi: 10.1007/s10639-020-10240-2

[22]. Mok, S. S., Tam, V. W., & Cheng, G. H. (2020). Exploring the cybersecurity awareness of primary school students in Hong Kong. International Journal of Environmental Research and Public Health, 17(16), 5771. doi: 10.3390/ijerph17165771

[23]. Mousa, F. T., Hassan, S., & Al-Salman, A. M. (2022). The impact of cybersecurity awareness on academic performance: A case study of a Saudi Arabian university. Education and Information Technologies, 27(1), 383-400.

[24]. National Cyber Security Alliance. (2018). Back to school: Securing the digital generation. Retrieved from https://staysafeonline.org/wp-content/uploads/2018/08/Back-to-School-Securing-the-Digital-Generation.pdf

[25]. National Cybersecurity Alliance. (2020). Cybersecurity Awareness Month: Tips for Educators. Retrieved from https://staysafeonline.org/wp-content/uploads/2020/08/CSAM-2020-Tips-for-Educators.pdf

[26]. Neumann, M. M., Neumann, D. L., Walker, R. A., & Baker, J. (2018). The effects of a digital citizenship program on the ethical and responsible use of technology in a rural school district. Computers in the Schools, 35(2), 95-110. doi: 10.1080/07380569.2018.1437517

[27]. Park, H. J., & Kim, J. (2018). The effects of cybersecurity education on elementary school students' awareness of cybercrime consequences. Journal of Educational Technology, 34(4), 617-630. doi: 10.17232/KSET.34.4.617

[28]. Philippine National Privacy Commission. (2020). 2020 Annual Report: Championing Privacy in the Time of COVID-19. Retrieved from https://www.privacy.gov.ph/wp-content/uploads/2021/01/2020-Annual-Report-2.pdf

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

[29]. Rennie, L. J., Phillips, L. G., &Quartly, J. (2017). Children's perceptions of cyberbullying: Examining gender, age, and grade differences. Journal of School Violence, 16(3), 270-288. doi: 10.1080/15388220.2016.1216221
[30]. Rosenblum, D. (2016). Cybersecurity in higher education. EDUCAUSE Review, 51(6), 13-14.
[31]. Simsek, E., & Akkaya, R. (2018). Effectiveness of digital literacy program on ethical and responsible use of technology in primary schools. Journal of Education and Practice, 9(22), 53-59.
[32]. So, H. J., & Lee, S. M. (2021). Parental mediation and online safety practices: Mediating roles of digital literacy among fourth-grade students in South Korea. Information, 12(2), 74. doi: 10.3390/info12020074
[33]. Sure, here's a sample review of related literature for the willingness to report suspicious activity as an indicator of cybersecurity awareness among Grade 4 learners:
[34]. Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257-285. doi: 10.1207/s15516709cog1202_4
[35]. Tondeur, J., van Braak, J., Ertmer, P. A., & Ottenbreit-Leftwich, A. (2019). Understanding the relationship between digital literacy and online safety for fourth grade students. Computers & Education, 142, 103641. doi: 10.1016/j.compedu.2019.103641
[36]. Vu, H. T. H., Nguyen, T. T. H., & Tran, V. N. (2021). Digital literacy and online safety practices of primary school students in Vietnam. Education and Information Technologies, 26, 2651-2668. doi: 10.1007/s10639-020-10495-9
[37]. Yıldız, R., Yıldırım, S., & Bozkurt, A. (2021). The effect of digital citizenship education on fourth grade students' ethical and responsible use of technology. Education and Information Technologies, 26(3), 2303-2319. doi: 10.1007/s10639-021-10545-y

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

APPENDIX A
INFORMED CONSENT

Dear Parents/ Guardians,

I am conducting a research study and I would like to invite your child to participate.

Before your child can participate, I need your consent. Please read the following statements carefully, and if you agree, sign the form below.

I (insert parent/ guardian name), am the parent/ and guardian of (insert child name), who is (insert age of child). I have read the description of the study provided to me. I understand the purpose of the study and what my child be asked to do.

I give permission for my child to participate in this research study.

I understand that my child's participation is voluntary, and that they may withdraw at any time without penalty or consequence. I also understand that my child's information will be kept confidential and anonymous, and that only the researcher and authorized personnel will have access to it.

If I have any questions or concerns about the study, I understand that I can contact the researcher.

Signature:_____Date:_____
Printed name:_____

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

APPENDIX B
SURVEY QUESTIONNAIRE

A. PART I. Cybersecurity Awareness

Source: National Cybersecurity Alliance. (2020). Cybersecurity Awareness Month: Tips for Educators. Retrieved from https://staysafeonline.org/wp-content/uploads/2020/08/CSAM-2020-Tips-for-Educators.pdf

Here is survey questionnaire to measure your cybersecurity awareness using a Likert scale ranging from "Strongly Agree" to "Strongly Disagree". There are three statements for each of the five indicators of cybersecurity awareness. To aware, use this scale:

5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree

A. Understanding cybersecurity concepts and terminology	**5**	**4**	**3**	**2**	**1**
1. I understand what a virus is and how it can infect a computer.					
2. I know what "phishing" means and how to avoid it.					
3. I am familiar with the term "encryption" and why it's important to use.					
B. Understanding cybersecurity concepts and terminology	**5**	**4**	**3**	**2**	**1**
1. I understand what a virus is and how it can infect a computer.					
2. I know what "phishing" means and how to avoid it.					
3. I am familiar with the term "encryption" and why it's important to use.					
C. Applying critical thinking to evaluate cybersecurity risks	**5**	**4**	**3**	**2**	**1**
1. I am able to identify when a website might not be safe to use.					
2. I think carefully before clicking on links or downloading files from the internet.					
3. I know how to tell if an email is fake or a scam.					
D. Applying critical thinking to evaluate cybersecurity risks	**5**	**4**	**3**	**2**	**1**
1. I am able to identify when a website might not be safe to use.					
2. I think carefully before clicking on links or downloading files from the internet.					
3. I know how to tell if an email is fake or a scam.					
E. Developing strategies for safe and responsible online behavior	**5**	**4**	**3**	**2**	**1**
1. I always use strong and unique passwords for my online accounts.					
2. I never share personal information, such as my home address or phone number, with people I don't know online.					
3. I always log out of my accounts when I'm done using them.					

B. PART II. Educational outcomes related to cybersecurity awareness

Common Sense Education. (n.d.). Digital Citizenship Curriculum. Retrieved from https://www.commonsense.org/education/digital-citizenship

Here is survey questionnaire to measure your cybersecurity awareness using a Likert scale ranging from "Strongly Agree" to "Strongly Disagree". There are three statements for each of the five indicators of cybersecurity awareness. To aware, use this scale:

5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

A. Applying critical thinking to evaluate cybersecurity risks	**5**	**4**	**3**	**2**	**1**
1. I think carefully about the consequences of sharing personal information online.					
2. I am able to identify when a website might be fake or fraudulent.					
3. I know how to assess the credibility and reliability of information found on the internet.					
B. Developing strategies for safe and responsible online behavior:	**5**	**4**	**3**	**2**	**1**
1. I always use secure passwords and change them regularly.					
2. I know how to set up privacy settings on my social media accounts to protect my personal information.					
3. I never engage in cyberbullying or other forms of online harassment.					
C. Using digital tools and resources ethically and responsibly	**5**	**4**	**3**	**2**	**1**
1. I know how to properly cite and attribute sources when using information found on the internet for schoolwork.					
2. I understand that downloading copyrighted material without permission is illegal.					
3. I never plagiarize or copy someone else's work without their permission.					

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1261

APPENDIX C
RELIABILITY ANALYSIS

Instrument	No. of Items	Cronbach's Alpha	Level of Reliability
Cybersecurity Awareness	15	0.701	Acceptable
Educational Outcomes	9	0.718	Acceptable
Overall	**24**	**0.711**	**Acceptable**