A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers

Principal Investigator
Dr. Angel Rathnabai

March 2023

विद्यया ऽमृतमश्नुते

एन सी ई आर टी
NCERT

Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Auribondo Marg, NCERT Campus, New Delhi, Delhi- 110016

A STUDY ON THE EFFECTIVENESS OF CYBER SAFETY AND SECURITY AWARENESS PACKAGE FOR TEACHERS

Research Report

Principal Investigator
Dr. Angel Rathnabai

Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Aurobindo Marg
New Delhi-110016

DECLARATION

I declare that this research entitled **"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers"** has been taken up as a part of the **PAC 20.25 project.**

Principal Investigator
Dr. Angel Rathnabai S
CIET-NCERT

Head (DICT)
Prof. Indu Kumar
CIET-NCERT

abehera

Joint Director
Prof. Amarendra P.Behera
CIET-NCERT

ACKNOWLEDGEMENT

We would like to sincerely thank Prof. Amarendra P. Behra, Joint Director, and Prof. Indu Kumar, Head, DICT & TD, Central Institute of Educational Technology (CIET), NCERT, New Delhi, for their valuable expertise and guidance throughout this project. Their leadership played a key role in shaping our work and ensuring its quality.

We also want to recognize the important contributions of the resource persons and experts whose insights and hard work were essential in the research.

I am also profoundly appreciative of the participants of the research. Their active engagement and enthusiasm were crucial in bringing this research to life. Their feedback and reflections provided valuable insights that have significantly contributed to the findings of this report.

Table of Contents

CHAPTER 1:INTRODUCTION

1.1 Background

In recent years, the rapid growth of technology and the growing reliance on digital platforms in education have highlighted the importance of strong cyber safety and security measures. Phishing attempts, ransomware events, and data breaches are among the cyber risks that schools and educational institutions are most vulnerable to. Teachers need to be sufficiently prepared to handle these difficulties and safeguard their pupils' online settings because they are frequently at the forefront of this digital landscape. In the classroom and online, teachers play an important role in educating and protecting students. They might not, nevertheless, have the requisite cyber security expertise to properly protect their own gadgets, information, and online identities. Teachers themselves, as well as their students and the larger school community, may be at risk due to this lack of cybersecurity awareness and training.

Studies have identified the necessity to create and assess teacher-specific cyber safety and security awareness programmes in order to solve this problem. These programmes are designed to equip educators with the necessary knowledge, resources, and tactics to recognise, address, and prevent cyber hazards. This will enable teachers to better safeguard their pupils, themselves, and their schools from the ever-present risks associated with the digital world. These crucial needs and the possible effects of such an intervention on enhancing teachers' resilience and understanding of cybersecurity would probably be the main topics of the study's backdrop on the effectiveness of the Cyber Safety and Security Understanding Package for Teachers.

1.1.1 Education in the Current Scenario

Technology has dramatically increased educators' teaching abilities. Online technologies such as Google Classroom and Zoom make it easier for teachers to conduct remote classes and communicate with students. Digital technologies for exams and grading save time and provide immediate feedback. Personalized learning technologies enable teachers to tailor lessons to specific students. Educational software provides a wide range of materials to make classes more engaging. Assistive technology benefits students with disabilities, ensuring that everyone can study effectively. Overall, technology has improved educational efficiency, effectiveness, and inclusion. Nowadays, teachers can profit greatly from cyber safety and security. Information is kept secure by them guarding student and personal data against unwanted access. Ensuring fairness in online tests and assignments is facilitated by these strategies that assist avoid cheating. Enabling safe communication routes with students and coworkers means that they are protected from cyber risks. The uninterrupted availability of online resources and instructional materials is another guarantee provided by cyber security. Keeping an online learning environment safe, it stops unwanted access to classes. Demonstrating a dedication to data privacy, it also fosters trust with parents, coworkers, and students. Teachers are able to concentrate on teaching successfully because cyber safety and security provide a dependable and secure learning environment. Teachers now face a number of risks to their online security and safety. Data breaches can result from hackers stealing student and personal information. It is dangerous to share information online due to the possibility of phishing attacks and malware-compromising communication channels. Lessons can be disrupted and the learning environment will be put in danger by unauthorized access to online classrooms. The educational process might be hampered by cyberattacks that destroy or restrict access to crucial instructional resources and materials. In order to safeguard both themselves and their pupils, educators must be on the lookout for these threats and implement robust cyber security protocols. In order to safeguard student and personal information, avoid disruptions to online learning, and maintain a secure learning environment, educators urgently require strong cyber safety and security measures.

1.1.2 Role of Teacher in the Current Scenario

Teachers are essential in transforming education, according to the National Education Policy (NEP) 2020. They have to put learner-centred pedagogies into practice, which shift from rote learning to more interactive, immersive methods catered to different student requirements. In order to improve instruction and provide individualized learning experiences, educators are adopting technology. This is especially important when it comes to supporting distance learning. They help children become more creative, critical thinkers, and problem solvers, preparing them for difficulties they will face in the real world. Teachers also promote holistic development by attending to the mental, emotional, social, and physical health of their students. They guarantee fair learning opportunities for all students, including those with impairments and those from marginalized backgrounds, by embracing inclusive education practices and flexible evaluation methodologies. Teachers support the goal of NEP 2020, which is to create an inclusive and responsive educational system that prepares children for the future, by working together, mentoring other educators, and interacting with parents and communities. In the case of cybercrime, educators are obliged to act quickly to minimize disruptions and guarantee that instruction continues. Teachers play a vital role in establishing a safe and secure online learning environment that supports NEP 2020 by raising awareness and enforcing norms around cyber safety. This helps students become prepared to navigate the digital world responsibly and safely.

1.1.3 Need for Cyber Safety and Security Awareness among Teachers

In the current digital era, ensuring that teachers have a strong awareness of cyber safety and security has become essential.

Teachers need to be more aware of cyber safety and security for a number of reasons:

Protecting Personal and Student Data: Instructors are in charge of handling private information such as attendance logs, grades, and personal information. Their comprehension of the significance of preventing breaches and unauthorized access to this data is aided by awareness.

Preventing Cyber Treats: By being aware of prevalent cyber dangers, instructors can take preventative measures against ransomware, malware, and phishing emails. They gain the ability to recognise dubious attachments, links, and fraudulent schemes.

Ensuring Safe Online Communication: Email, messaging applications, and online platforms are frequently used by teachers to connect with children, parents, and colleagues. They can secure these channels and uphold professional communication standards by being aware of potential data leaks.

Securing Digital Teaching Resources: Lesson plans, tests, and instructional resources are becoming more and more digital. To maintain uninterrupted instruction, teachers must protect these materials from unwanted access and guarantee that they remain accessible.

Upholding a Reliable Learning Environment: Students' learning experiences can be negatively impacted by cyberattacks that disrupt online classrooms and compromise educational platforms. Teachers who are aware of the importance of security can take action to protect digital classrooms and learning resources.

1.2 Statement of the Problem

The purpose of a study on the effectiveness of a cyber safety and security awareness package for teachers is to assess how well-specialized training may improve educators' understanding of and proficiency in safeguarding student information, preventing cyber threats, and maintaining a safe online learning environment. This study intends to ascertain how well the awareness package has prepared teachers in various schools in India to navigate and effectively reduce cyber dangers in educational environments.

In this context, the current research work has been undertaken and is entitled *"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers"* has been taken up.

1.3 Operational Definition of the Key Terms

1.3.1 Cyber Safety and Security

According to Merriam-Webster, cyber safety is the safe practices when using the Internet to prevent personal attacks or criminal activity. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks(Kaspersky,2024). In this study Cyber Safety and Security refer to teachers who understand how to keep themselves and their students safe online and are practicing cyber safety and security. It involves educating students on how to be responsible online, accessing the internet safely, creating strong passwords, and identifying and addressing online threats including scams and cyberbullying.

1.3.2 Awareness

"Awareness is the quality or state of being aware : knowledge and understanding that something is happening or exists" (Merriam-webster, 2024). In this study an awareness for teachers is referred to as an organized educational programme designed to give instructors the knowledge, skills, and practices they need to comprehend and apply cyber safety and security measures in learning environments.

1.3.3 Teachers

According to Merriam-Webster, a teacher means “someone whose job is to teach in a school or college”. In this study, teacher refers to an individual who is employed in an educational institution and is responsible for delivering instruction and guidance to students.

1.4 Variables of the Study

- **Independent Variable**

Variables that have undergone manipulation are considered as independent variables. A variable that modifies to observe how it impacts another component is known as an independent variable. So, in this study, Gender is considered as an independent variable.

- **Dependent Variable**

A dependent variable is the measured or observed variable. This study tries to find out how the dependent variable is affected by the independent variable. In this study, the awareness on cyber safety and security is considered as the dependent variable and the study intends how the awareness varies across the selected independent variables. By observing the dependent variable, the effect of the independent variable can be measured. It was tested whether the independent variable would have an effect on the dependent variables i.e., ‘Awareness package’ on Cyber Safety and Security for Teachers.

1.5 Research Questions

1. What is the awareness level of teachers on cyber safety and security?
2. What are the dimensions in which teachers lack awareness of cyber safety and security?

1.6 Objectives of the Study

1. To study the awareness package of teachers on cyber safety and security.
2. To study the difference in awareness packages on cyber safety and security among teachers with respect to various subgroups.
3. To study the difference in different dimensions of cyber safety and security awareness packages among teachers with respect to various subgroups.

1.7 Hypothesis of the Study

To undertake a meaningful analysis, the following hypotheses were proposed.

H_1: There is no significant difference in the pre-test and post-test scores on cyber safety and security awareness between male and female teachers.

H_2: There is no significant difference in the pre-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety

- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_3: There is no significant difference in the post-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues in the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_4: There is no significant difference between male and female teachers in their pre-test scores with regard to the Concept of Cyber Safety and Security domain.

H_5: There is no significant difference between male and female teachers in their pre-test scores with regard to the Device Safety and Security domain.

H_6: There is no significant difference between male and female teachers in their pre-test scores with regard to Browser, Email Security and Digital Financial Security domains.

H_7: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social Media and Safety domain.

H_8: There is no significant difference between male and female teachers in their pre-test scores with regard to the Cyber Scams and Frauds domain.

H_9: There is no significant difference between male and female teachers in their pre-test scores with regard to the physical and psychological domains.

H_{10}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{11}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Legal Frameworks for the Cybersecurity domain.

H_{12}: There is no significant difference between male and female teachers in their post-test scores with regard to the Concept of Cyber Safety and Security domain.

H_{13}: There is no significant difference between male and female teachers in their post-test scores with regard to the Device Safety and Security domain.

H_{14}: There is no significant difference between male and female teachers in their post-test scores with regard to the Browser, Email Security and Digital Financial Security domain.

H_{15}: There is no significant difference between male and female teachers in their post-test scores with regard to the social media and safety domain.

H_{16}: There is no significant difference between male and female teachers in their post-test scores with regard to the cyber scams and frauds domain.

H_{17}: There is no significant difference between male and female teachers in their post-test scores with regard to the Psychological Issues In the context of Cyber Safety and Security domain.

H_{18}: There is no significant difference between male and female teachers in their post-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{19}: There is no significant difference between male and female teachers in their post-test scores with regard to the legal framework for the cybersecurity domain.

1.8 Research Methodology

1.8.1 Research Design

Research design is defined as a framework of methods and techniques chosen by a researcher to combine various components of research in a reasonably logical manner so that the research problem is efficiently handled. It provides insights about "how" to conduct research using a particular methodology. Every researcher has a list of research questions which need to be assessed – this can be done with research design. The sketch of how research should be conducted can be prepared using research design (Khanday, 2019). According to Joseph Chacha (2021), a research approach refers to the structure, methodology, or strategy employed to get answers for a research issue.

The study used a survey method, a quantitative research technique that optimizes descriptive and inferential statistics, to look into teachers' awareness of cyber safety and security at the national level. This method has been selected since the intention of the study was to explore the current level of awareness of teachers about cyber safety and security. The survey research helped the researcher to get an insight about the prevailing level of teachers' awareness about cyber safety and security across the nation.

1.8.2 Population of the Study

The population of the present study is all the Teachers, Teacher Educators, Administrators and educational stakeholders from various States/ UTs and Autonomous Organizations like CBSE/ KVS/ NVS/ AEES/ Sainik School/ CISCE/ EMRS. The target group also includes Teachers, Administrators and Faculty of various constituent units of NCERT like DMS, RIEs, NIE, and PSSCIVE from all 28 Indian States and 8 Union Territories. There are about 16 million teachers in the 2022-23 session (MoE, 2022) and all of them were considered as the population of the present study.

1.8.3 Sample of the Study

In order to conduct the research, purposive sampling was done. Twenty (20) teachers/ teacher educators were selected from each state/ UT, 100 participants representing CBSE and 5 each from other autonomous organizations. A total of 950 participants were requested to be deputed but a total of 470 individuals participated in this research study.

1.8.4 Sampling Technique

Multi-stage sampling was used to collect data from all state board-affiliated schools and CBSE schools. The first stage was the selection of states/UTs for collecting data and in the second stage, it was decided to collect data from teachers in all boards i.e., state board affiliated schools and CBSE schools from all 36 States/UTs. Next, the schools were selected based on their types i.e. Government, Aided and Private schools from all 36 States/UTs. All the schools affiliated to the state board are considered as Government and Aided schools and all the schools affiliated to the CBSE are considered as Private Schools.

1.8.5 Research Tool

A cyber safety and security awareness scale covering four dimensions of cyber safety and security was constructed. Validity and reliability was achieved by going through pilot testing. The research tool was developed in English and also translated into Hindi.

1.8.6 Data Collection

An online-based survey was used to collect the data. Permission from the school authorities/Chairpersons of Autonomous Bodies under the MoE, MoD, MoTA, Principals of SCERTs/ SIEs in the States/UTs, Principals of RIE and school Heads of DMS was obtained and Consent was obtained from the teachers for the data collection. The research tool was shared through the school authorities and in turn data was collected from the teachers.

1.8.7 Data Analysis

The quantitative data was analyzed under descriptive and inferential parameters. MS Excel was used for descriptive analysis, and SPSS Software was used for inferential analysis, such as independent sample t-test.

1.9 Need and Significance of the Study

Digital technology now plays a crucial role in education, presenting both possibilities and difficulties. The growing threat of cyberattacks on educational institutions is one of the most urgent issues. Schools are increasingly becoming targets for cyber threats like phishing, ransomware, data breaches, and online harassment as a result of the growing use of digital technologies in the classroom. In order to safeguard themselves, their students, and the school's digital assets, teachers - who are at the forefront of this digital shift—must be knowledgeable about cyber safety procedures.

Despite the crucial significance of cyber safety, a large number of teachers lack adequate training in this domain, which renders them severely lacking in their capacity to properly manage and secure digital information. This lack of readiness may leave gaps that could lead to harmful assaults on private student and school data. Teachers must be aware of these standards in order to guarantee compliance and safeguard sensitive data, as educational institutions are subject to strict privacy and data protection laws.

Yet another important factor that motivates this study's necessity is student safety. Instructors need to be prepared to teach and shield their students from cyberbullying, online harassment, and other online dangers because they are the ones who shape students' online conduct. The increasing prevalence of digital technologies in education necessitates the promotion of safe and secure technology use inside the academy.

"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers" is significant in a number of ways. Its primary goal is to assess how well the cyber safety and security awareness package has improved teachers' knowledge of and use of cyber safety. Teachers that are more proficient in this area will be able to better manage digital settings, which will improve school security as a whole. Second, by giving educators the skills they need, the study contributes to the protection of school networks and data against cyberattacks, guaranteeing a safe learning environment.

Furthermore, policy formation is affected by the study. Researchers' findings can provide policymakers and educational authorities with information that will help them create comprehensive cyber safety regulations and teacher-specific training programmes. The larger objective of establishing a safe learning environment and encouraging confidence and trust among children, parents, and the larger school community is thereby supported by this.

Additionally, the study helps to lower the prevalence of cyberbullying and other cybercrimes by strengthening instructors' capacity to teach pupils about safe online practices, which fosters a healthy digital culture in schools. Finally, as technology develops further, instructors will be better equipped to meet new difficulties by receiving continual training and knowledge in cyber safety, which will ensure the long-term security and resilience of educational institutions.

This study concludes by addressing the urgent need for instructors to become more knowledgeable about cyber safety and security. It seeks to establish a safer, more secure learning environment for all parties concerned by assessing and enhancing the awareness package's efficacy and making sure that educators are equipped to handle the challenges of the digital era.

1.10 Scope of the Study

"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers" aims to address a number of important issues in light of the growing use of digital technology in education. The study covers a wide range of geographic areas, including states, union territories, and suburban and rural areas (UTs). It encompasses independent organizations like KVS, NVS, AEES, CBSE, and EMRS-NEST in addition to schools falling under other administrative classifications like government, private, and aided schools. Teachers from all grade levels, teacher educators, and school administrators make up the participant demographics. This offers a thorough grasp of cyber safety awareness for various jobs in the educational ecosystem. The awareness package that is being evaluated consists of training sessions, seminars, instructional materials, and useful guidelines that address protecting student privacy online, identifying and addressing cyber threats, and comprehending digital citizenship.

The study will focus on changes in knowledge, attitudes, and practices related to cyber safety in order to gauge the efficacy of the awareness package through pre and post-training assessments, and surveys. Along with their application in the classroom, it will evaluate these techniques' long-term sustainability. Furthermore, this research will investigate the wider implications of improved cyber safety knowledge for the educational setting, including enhanced digital security procedures, a decrease in cyber accidents, and a rise in instructors' and students' self-assurance in using digital resources securely.

Educational policymakers, administrators, and training institutions will find great value in the study's conclusions. It will be suggested that curricula and professional development programmes for teachers incorporate cyber safety training. In order to keep up with changing cyber threats and technical breakthroughs, the study will also include recommendations for tactics for ongoing enhancement and upgrades to the awareness package. This study's overall goal is to improve instructors' awareness of cyber safety and security while also fostering a safer, more secure learning environment.

1.11 Delimitations of the Study

Delimitations help focus the research by specifying what aspects will be included and excluded from the investigation. Here are some probable delimitations for this study:

- **Dimensions of Cyber Safety and Security:** The study concentrated only on four dimensions of cyber safety and security namely Physical-Psychological, Legal, Socio-ethical, and Technical and concept of cyber safety. This boundary guarantees a targeted analysis of the most critical cyber safety and security concerns that affect the intended sample.
- **Research Methodology:** To investigate teachers' awareness of cyber safety and security, the study used specialized research techniques, such as online surveys through Google Forms.
- **Language coverage:** The tool of the study was prepared in English and translated into Hindi only.

1.12 Organization of the Research Report

The research report is organized into six chapters. The first chapter, Introduction, presents the need and significance of the study, statement of the problem, the definition of the key terms, variables of the study, objectives of the study, the hypotheses of the study, methodology, scope and delimitations of the study. The second chapter is a review of related literature, a theoretical overview and studies related to cyber safety and security. The third chapter, Methodology, presents a detailed account of the methodology, including descriptions of the method of the study, design of the study, variables of the study, tools used for the study, description of tools, population and sample selected for the study, procedures for data collection and the statistical techniques used for analysis. The fourth chapter, Analysis and Interpretations, deals with the analysis of data in detail. This chapter includes preliminary analysis, percentage analysis, mean difference analysis, correlation analysis, regression analysis, and thematic analysis. The fifth chapter, Summary of Findings and Conclusions, contains a summary of findings, tenability of hypotheses, the relationship of results to existing studies, limitations of the study, suggestions, recommendations and educational implications for further research, and conclusions.

CHAPTER 2:REVIEW OF RELATED LITERATURE

2.1 Introduction

A scientific attempt to broaden the boundaries of human comprehension, research is fundamentally a continuous conversation. Before beginning any investigation, a thorough examination of the ongoing discussion is important. Here, the literature review assumes a central role, serving as a link between existing knowledge and forthcoming research. Its significance cannot be emphasized since it provides a solid basis for thorough study and has many advantages. Examining the body of prior research is essential when it comes to educational research since it serves as the foundation for novel and vital findings. Examining relevant literature is a crucial first step, compass, and guidance for academic research projects. First of all, it provides a thorough grasp of the existing environment, including recognized gaps, accepted ideas, and established information. In addition, this enables ongoing research to place the findings within the broader discussion carefully. Moreover, a critical examination of earlier research refines the methodology by highlighting both possible advantages and limitations. It also generates new ideas by pointing out places where the body of knowledge is lacking or ambiguous, which opens the door for special contributions. In the end, a comprehensive study promotes scholarly progress within an area. The following are the reviews from the national and international research studies which were carried out on awareness on cyber safety and security among teachers.

2.2 Review Related Literature

Abbas Moallem (2018) This study reports the preliminary findings of a study designed to investigate student awareness and attitudes toward cyber security and the risks that result in the most advanced technological environment: Silicon Valley in California, USA. Silicon Valley's student body is extremely ethnically diverse. The goal was to see how well students in such a technologically advanced environment are aware of cyber-attacks and how they protect themselves against them. Early statistical analysis suggested that, despite their belief that they are being watched when using the Internet and that their data is not secure even on university systems, college students are not well informed about how to protect their data. Furthermore, it appears that educational institutions are not actively working to raise awareness among college students about these issues and how to protect themselves from potential cyber-attacks such as identity theft or ransomware. According to the findings of this survey, college students, despite their belief that they are being watched while using the Internet and that their data is not secure even on university systems, are still unaware of how to protect their data. They reported, for example, low levels of two-factor authentication usage or password complexity for accounts. Furthermore, it appears that educational institutions are not actively working to raise awareness among college students about these issues and how to protect themselves from potential cyber-attacks such as identity theft or ransomware. According to reports, most students are aware of the risks of providing personally identifiable information to an entire university population, such as identity theft and stalking, but still feel comfortable doing so.

Abdilkadir Hussein Elmi (2019) The study's goal was to examine university students' awareness of cyber security in Mogadishu by focusing on various security threats on the internet. This study used one-way analysis of variance (ANOVA) to determine whether or not there is a difference in Cyber Security Awareness among graduate and undergraduate students at five well-known universities (i.e. Simad, SIU, Uniso, Jamhuruya and Mogadishu). The study also used the questionnaire method to collect data, and it included 250 graduate and undergraduate students from five well-known universities (i.e. Simad, SIU, Uniso, Jamhuruya and Mogadishu). This study discovered that the cross-tabulation (universities where you meet the most types of attacks, in which Simad and Jamhuruya students suffer virus attacks while having no problem with phishing, password strength, and password strength) Furthermore, for every ten students in Simad, nine suffer virus attacks, whereas for every eleven students in Jamhuruya, eleven suffer virus attacks. In terms of SIU students, they are free from others in terms of password strength and social network misuse. In contrast, Mogadishu students are subjected to both virus attacks and phishing while remaining immune to others. Finally, Uniso is immune to both virus attacks and password strength. The ANOVA Table comparison of five universities shows that there is a statistically significant difference in cyber security between the five universities, with a P.value of less than 5%. F (245, 4) = 11.185, p = 0.0000 As a result, the study rejected the null hypothesis that there is no difference in cyber security between the five universities and concluded that there is a statistically significant difference in cyber security between the five universities, which confirmed the cross-tabulation result.

Adamu Abdullahi Gabra et.al. (2020) This Case Study presents the preliminary findings of a quantitative survey conducted in Nigerian universities to assess students' awareness and enthusiasm for learning cybersecurity. The survey's goal was to determine how students in this developing country are aware of cyberattacks and how they can mitigate them, as well as whether a cybersecurity awareness programme is part of the University programme. According to preliminary findings, the students claimed to have basic cybersecurity knowledge but are unaware of how to protect their data. Furthermore, it appears that most universities lack an active cybersecurity awareness programme to improve students' knowledge of how to protect themselves from any threats. Students who were polled expressed an interest in learning more about cybersecurity.

Ahmad et.al. (2020) The purpose of this study was to determine the level of awareness of social media use on safety issues among youths. The survey-based study employed frequency (frequency), percentage, mean score, and interpretation. The sample consisted of 205 randomly chosen youths from Tun Hussein Onn University Malaysia (UTHM). This study's data was analyzed using the Statistical Package for the Social Sciences (SPSS) version 21. The findings revealed that youth were unaware of the prevalence of social media use. Furthermore, the correlation coefficient did not show a significant relationship between social media usage and student awareness of social media, but rather a low value.

Aminu Aliyu et.al. (2021) Incorporating cybersecurity into university curricula is critical for assisting students in remaining safe while using the Internet and social media. Today, there is a lot of emphasis on understanding cybersecurity concepts, as well as the efforts of government and institutions to help introduce cybersecurity as an independent degree programme and other related disciplines. Several bodies (such as NITDA, NCC, NCS, and CPN) and scholars developed workshops, seminars, and conferences, and guidelines were developed and disseminated to raise cybersecurity awareness. A survey of nine tertiary institutions in Kaduna, Kano, and Sokoto was conducted for this study. A systematic convenient sampling technique was used to select 100 respondents from each institution (universities, polytechnics, and colleges of education). The data collected from the paper and pen questionnaire on the students' cybersecurity awareness was analysed using SPSS v17 software. Significant findings revealed that the majority of students are aware of cybercrime and threats. Furthermore, the findings revealed that most students are careless about changing their passwords on a regular basis, but are concerned about creating strong passwords. When they leave, many students lock their computers with a password. In addition, the findings revealed that many students are less vigilant against virus attacks. However, the majority of people are aware of the risks of disclosing personal information and location on social media. Finally, it is recommended that all stakeholders take proactive measures to protect themselves, their data, and their network infrastructure from cybercrime or threats.

Anastasios Papathanasiou et.al. The increased use of personal computers and other Internet-capable devices, as well as the availability of public WiFi hotspots, enabled people to make extensive use of the available Internet services, making them a tempting target for cybercriminals. Furthermore, cybercrime is transnational in nature and can affect individuals in different geographical locations at the same time, necessitating international cooperation in order to be effectively combated. This paper describes the various international efforts against cybercrime in which Greece participates, as well as the relevant legal framework and some future developments.

Anderson, Sweeney y Williams (2011) The purpose of this paper is to investigate the cyber security deficiencies that freshman university students in Information Technology (IT) undergraduate programmes have, and assess the impact of an awareness and training programme designed for them. One group of students took part in this study; they were surveyed before and after a training activity that was presented to them as a conference. The participants' responses were analyzed using SPSS statistical software, and several non-parametric tests were run to look for differences before and after the event. It was discovered that participants could have higher levels of knowledge and safety in their daily activities; additionally, it was discovered that the conference increased their perception about cyber-security concepts and awareness to create information backups more frequently. These preliminary findings indicate a positive effect, which encourages the implementation of a continuous training and awareness programme.

Arwa A. Al Shamsi (2019) The purpose of this study is to look into the effectiveness of the cyber security awareness programme offered by the Ministry of Education in the UAE to students aged 8 to 10. This research paper's methodology was based on qualitative data collection methods, with data collected from interviews with both programme trainers and students who attended the programme. It was discovered that children may be exposed to various online risks, and the topics included in the cyber security awareness programme were effective and aligned with potential online risks to which children may be exposed. Both the trainers and the students agreed that the cyber security awareness programme was effective, and the students believed that the programme influenced their online behaviour. Although the interviews yielded useful information, the true effectiveness of the cyber security awareness programme is difficult to assess because it is dependent on how students behave online.

Bandara I. et.al. Cyberspace is the term for the Internet's limitless realm. The set of regulations established for the protection of this cyberspace is known as cyber security. Numerous studies have shown that e-learning systems are being used more and more, and this trend is only expected to continue. However, neither research nor education have paid much attention to the issue of e-learning system security. As it applies to e-learning systems, it has been demonstrated in this work as a method for analyzing, evaluating, monitoring, measuring, and managing cyber security. The security of e-Learning systems offers a special issue because thousands of users across hundreds of networks access and manage a variety of systems over the Internet. The prevalence of internal cyberattacks and the inadequate IT policies and procedures in e-learning systems are also revealed in this study, given the standard architecture and the unique security requirements of these systems. The paper also discusses the most significant security challenges that may be pertinent for open, distributed, and interconnected e-learning systems. As a result, security poses a significant challenge in ensuring that interested and authorized actors only have access to the appropriate information at the right time.

Breda F (2017) People, as individuals, are more vulnerable today than ever before as the digital era matures, cyber security evolves, and software vulnerabilities diminish. Currently, one of the most common and effective penetration attacks is social rather than technical, and these exploits are so effective that they support the vast majority of cyber-attacks. Social engineering is the practice of exploiting human flaws to achieve a malicious goal. In the context of information security, practitioners breach defences to gain access to sensitive data, taking advantage of the human tendency to trust. Cybercriminals persuade their victims to violate security protocols, exposing confidential information that could be used in a more targeted attack. Unfortunately, in many cases, targets are manipulated to unintentionally infect and sabotage the system. This paper investigates common social engineering techniques used by attackers while also revealed a fundamental complementary technical methodology for conducting effective exploits.

Challiz D. Omorog and Ruji P. Medina (2018) This study looks at how Filipinos see internet security in order to show how urgently the government has to develop a cybersecurity culture for all Filipinos. A two-page questionnaire including fundamental demographic data and two crucial topics, internet usage and security policies, was used to interview 252 respondents utilising traditional, online, and phone methods. According to the results, there has been a significant rise in internet users over the past three years (by 50%), and the majority (94.4%) access the web via a mobile device. Despite the fact that 94.4% of people access the internet most often at home, a sizable portion (38.9%) have been using free WiFi access points in restaurants (11.1%), malls (22.2%), and other public spaces (38.9%) to use internet services (email and downloading) that are susceptible to cyberattacks. The survey also showed that although respondents may have had some familiarity with Internet security software, there is very little proper deployment.

Dambrosio, R. (2021) This qualitative study aimed to investigate the gaps in teachers' understanding of cybersecurity, cybersafety, and cyber ethics, or C3, as well as to better understand instructors' self-efficacy to alert pupils of the online hazards that can endanger personal information. Among the participants were five middle school instructors from a tiny Californian district located in the Central Valley. For the aim of gathering data, the participants took part in a 40–50 minute interview. Three topics emerged from the data analysis: the perceived significance of C3 issues, the knowledge gaps surrounding C3 issues, and the implications of online student information protection for instructional methods. The results of this survey indicate that while participants believe that student online safety and security are vital, they do not have the appropriate understanding to effectively educate C3 problems.

Deepalakshmi (2019) Sharing information among the student body is an important avenue. Social networks play an important role in the rapid dissemination of information. Different types of college students were interviewed in this exploratory study to assess the impact of smartphone, Facebook, Twitter, LinkedIn, and WhatsApp use. The general public's knowledge of software use and installation is also polled. Security measures in the system and mail usage are also investigated. The value of user-generated information differs significantly from that of abuse and spam. As the availability of such information grows, the goal of identifying high-quality information in user-contributed sites—social media sites—becomes even more important.

Elradi and Abaker (2020) The paper focused on evaluating cyber security awareness among students and faculty members at a Sudanese college, emphasizing trust, password management, and defensive attitudes. Conducted through a survey, the study included 200 students and 100 faculty members, with a gender distribution of 56% males and 44% females. Findings indicated a generally low level of security awareness across all participants, with weak defensive behaviors insufficient to protect individuals or the institution. Faculty members demonstrated slightly better cyber security knowledge, scoring 8% higher than students. These results highlight the critical need for targeted training strategies to address identified security gaps and improve overall cybersecurity practices within the college community.

Faisal Amir et.al. (1999) One traditional way of teaching and learning is in the classroom. A normal lecture that refers to an established item, idea, or theory frequently leaves the student struggling and longing for a review of the fundamentals. Students find it difficult to absorb new concepts because of the necessary time constraints, restriction of fundamental concepts, and absence of interactive training tools. Cyberlearning, which includes knowledge from linked websites, student-student chatting, and online teacher-student interaction, is still a relatively new idea. Coherent analysis and well-articulated, well-reasoned thoughts on key subjects are produced in an environment where people from diverse backgrounds can express their differing points of view on complicated issues. Interaction in cyberspace can undoubtedly aid in the reformation, enhancement, and expansion of high-quality education. This article discusses interactive campus technology, infrastructure, and deployment, as well as distance learning strategies. A special focus has been placed on developing nations where financial limitations are the main barrier to technological adoption. The currently popular online distance learning strategies are described together with an overview of their evaluation. This paper's main theme was the idea of ubiquitous computing in the future, both on and off campus. This idea needs to be developed by gathering real-time statistical information from students in various grades. The mentioned concept calls for greater faculty involvement, the creation of online and interactive lectures using Mentors, the provision of infrastructure to support the notion with a focus on the superiority of offline Mentors, and updated FAQs. The study provides a general overview of the fundamental requirements and constraints of common higher education online learning and teaching models. Moreover, the study highlights the advantages and restrictions of using distance learning for fundamental services like classes, seminars, and tutoring. A novel idea of learning has been presented, showing how a student might gain knowledge while simultaneously acting as a teacher and a learner.

Fariza Khalid et.al. (2018) Nowadays, people are more susceptible to online threats due to the emergence of numerous online applications and the widespread use of social media. Online users run the risk of encountering racial abuse, cyberbullying, online fraud, gaming and gambling addiction, and pornography on a daily basis. It takes self-awareness to safeguard oneself against these threats. The purpose of this study is to look into college students' knowledge about cybersecurity. A collection of questionnaires administered to 142 second-year education faculty students at one of Malaysia's institutions served as the method for gathering research data. Using SPSS software, descriptive data analysis was carried out. The study's findings revealed that while these college students had a high degree of awareness regarding several aspects of cyber security, such as cyberbullying, personal information, and internet banking, they lacked the necessary information regarding the topic of cybersex and self-protection. The importance of the entire community in educating youngsters and young people on this subject is also covered in this essay.

Frank Cremer et.al. (2022) A systematic review of studies on cyber risk and cyber-security databases was conducted in this paper. The majority of the datasets were discovered to be in the field of intrusion detection and machine learning and are used for technical cybersecurity aspects. The available datasets on cyber risks were underrepresented. Assessing and understanding cyber risk is a major challenge for cyber insurance stakeholders due to its dynamic nature and lack of historical data. To address this challenge, more cyber data density is required to assist cyber insurers in risk management and researchers with cyber risk-related topics. Mandatory reporting of cyber incidents could help improve cyber understanding, awareness, and loss prevention among companies and insurers, according to 'Open Science' FAIR data (Jacobsen et al. 2020). Cyber risks have become better understood as data has become more widely available, allowing researchers to conduct more in-depth research into these risks. To reduce cyber risks, businesses could incorporate this new knowledge into their corporate culture.

Ibrahim Usman and Abdullah Mat Rashid (2014) The primary goal of this study is to assess pre-service teachers' safety awareness in technical and vocational education. This study focuses on tool and equipment arrangement, the use of personal protective devices, and years of programme study in terms of safety awareness. This study used a survey that was given to 196 Malaysian technical and vocational pre-service teachers. The findings show that pre-service teachers have a moderate level of safety awareness, tools, and equipment arrangement.

Meanwhile, the findings show that there are significant differences in safety awareness between the years of study of pre-service teachers.

Karagozlu, D. (2020) Cybersecurity worries grow along with the rate of cyberattacks. It is possible to secure the online environment and user rights by using a variety of tools, policies, security ideas, security measures, risk management strategies, activities, education, applications, security, and technologies. The objective of this study is to ascertain how pre-service teachers behave with relation to cyber security, hence the goal of this study was to ascertain how pre-service teachers behave. The Personal Cyber Security Ensuring Scale was utilised in this study, which was created using the quantitative research approach. The study involved 144 pre-service teachers from two separate universities who enrolled in instructional technology and material design courses during the spring 2019–2020 semester. Although the participants occasionally took action to leave no trace, take precautions, and safeguard personal privacy, it has been discovered that they regularly took action when they encountered untrustworthy persons and situations in the online world.

Kerryann Walsh et.al. (2020) This study was conducted to aid in the development of a best practice framework for online safety education in Australian schools ranging from Foundation to Year 12. This framework aims to provide a consistent, overarching national narrative for education that includes state and local perspectives. Territory education departments, Catholic and independent school systems, and external online safety are all examples of these providers of education. It offers a well-defined set of broad components as well as a subset of meaningful indicators that are easily applicable to online safety education practice. The framework is comprehensive enough to be implemented for future online safety education initiatives, and to differentiate specific programme quality.

Ljupco Sotiroski (2018) This paper aims to present important elements that have a strong impact on the level of cooperation, confidence, and awareness of subjects involved in the public and private environments who share the need and necessity for cooperative security protection of critical infrastructure. With the advancement of information and other technologies, society has become more complex and vulnerable. The world is facing high risks, particularly in terms of cyber threats and consequences. The complexity of the corporate security process identifies and implements all necessary legal measures to manage security risks. Crime, facilitated by network and computer technologies, has evolved into cybercrime, and war, in turn, has evolved into cyberwar. Cybercrime, cyber war, and cyberterrorism are examples of emerging phenomena that must be addressed by law. Effective legal regulation presupposes the development of a viable policy that can adequately address the substance of the problem as well as its technical complexity on multiple levels, such as legislative interventions in the form of criminalization and harmonisation, international cooperation, collaboration with the private sector, professional educational and capacity building in terms of technical support and assistance. Many countries, particularly developing ones, lack criminal laws that specifically address cybercrime. They also lack the capacity to enforce the laws. In terms of cyber threats and prevention, developing countries continue to face legal gaps. Cyber risks manifest on multiple levels, both national and international. The common umbrella concept of cyber security describes these concerns collectively. A legal framework, as well as adequate regulations and implementation, are required to protect against cyber threats.

Lohote Prathamesh Yashwant (2021) According to a review of the selected literature, the IT industry has been playing catch-up with hackers and cybercriminals for decades. Thus, there is a need for a cyber-security curriculum in the near future to instill cyber-security understanding in today's youth, and the IT sector will eventually gain more profound, securely skilled professionals. It was discovered that protecting children through cybersecurity education is critical so that they are aware of the potential risks they face when using internet communication tools such as social media, chatting, and online gaming. However, cybersecurity education faces a number of challenges. These include teacher knowledge levels, as well as a lack of expertise, funding, and resources. All relevant parties, including teachers, parents, peers, and the government, must collaborate to find the best solution for protecting children from cybercrime and cyberbullying through school-based cybersecurity education. Because cybersecurity campaigns are more interactive and interesting for children to understand, the media, such as television and radio, must also play an important role in educating children through cybersecurity campaigns. Hence Effective cyber-security policies, best practises, and, most importantly, implementation at all levels are required. The participation of the government and education systems in the cyber security awareness approach will lead to a more secure nation in the future.

Lydia I. Eleje et.al. (2022) Numerous studies have documented the increasing use and continued growth of e-Learning systems, but little attention has been paid to cyber-security issues in digital assessment. Research and education are scarce about lecturers' perspectives on the impact of cyber-security issues in digital assessment on assessment outcomes. This research gap was the focus of the current investigation. As a result, descriptive survey research was carried out with 200 lecturers from the education discipline of government-owned degree-awarding tertiary institutions in Anambra state, Nigeria. An 8-item questionnaire created by the researchers was used to collect data. In order to answer one research question and two hypotheses, descriptive and inferential statistics were used in the data analysis. There were significant differences in lecturers' perspectives on the impact of digital-assessment security issues on students' assessment outcomes based on level and cadre, but not on gender. Cyber-security issues in digital assessment have a negative impact on students' assessment outcomes, which are heavily influenced by academic level and cadre. More research is needed to confirm the consistency of the findings and determine whether the relationship is causal.

Madhulika Singh and Arun Kumar Singh (2014) This essay discusses numerous forms of cybercrime as well as the laws that can be used to combat them as well as security advice. One of the most important conclusions to come out of this research was that malicious software and hackers love to hang out on the Internet. It's crucial to keep in mind that responding to email advertisements is never a good idea. You should also only visit websites that you are familiar with or have bookmarked, and you should always check the address before continuing your search. Use a genuine operating system that is regularly updated through the internet, according to the study. Using a combination of alphabetic, numeric, and special characters, create a strong password. Never click on links that are sent via email or chat. It might be a virus or a link that can steal cookies.

Mamata Joshi and Asmita Udpikar (2014) study focused on cybercrime and security prevention in relation to the Internet, which is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users globally. The Internet transports a vast array of information resources and services, such as the World Wide Web's (WWW) interlinked hypertext documents and the infrastructure to support electronic mail. Cybercrime has evolved at an astounding rate, mirroring the inevitable penetration of computer technology and communication into all aspects of life. While society has been inventing and evolving, criminals have demonstrated remarkable adaptability in order to reap the greatest benefit from it. To avoid giving cybercriminals the upper hand, those fighting cybercrime must try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods accordingly.

Maria Bada and Jason R. C. Nurse (2019/20) As online threats and cyber-attacks become more prevalent on the Internet, a community must develop a better understanding of these issues and how they can affect lives. This study took a significant step toward that goal by investigating how members of the public perceive and engage with risk, as well as how they can be impacted following a cyber-attack. The study concentrated on the social and psychological consequences of attacks because they are frequently overlooked in research and practice. These are, however, critical factors in improving an understanding of the broader impact of an attack. The research examined two well-known cyber-attacks in the context of the breadth of outcomes to ground our work. This study is expected to inspire others to conduct additional research in this area and the interaction between cybersecurity and cognitive factors.

Maria Bada et.al. (2015) paper focuses on cyber security awareness campaigns and seeks to discover critical security-related variables that could prevent them from successfully altering people's behaviour. The anticipated results have not been achieved despite past and present attempts to enhance information security procedures and advance a sustainable society. In this paper, psychological theories are utilised to examine awareness and behaviour in the field of cyber security while also conducting a focused analysis of recent work. The goal is to make a first step toward a better understanding of the factors contributing to the difficulty of modifying cyber security behaviour. The study also reveals a wide range of psychological theories of behavioural modification that can be applied to dramatically increase the effectiveness of information security awareness campaigns.

Mika Karjalainen (2019) Cyber security exercises (CSE) are complex learning experiences that use simulation to develop expert knowledge and competence. This paper investigated pedagogical issues concerning CES, ranging from exercise design to training results and evaluation. Furthermore, the study presents a Deliberate Practice-oriented perspective on expert and competence development for CSEs. The study collected field notes, observations, questionnaire results, and other documentary data while organizing these training events, and the data used was gathered from multiple CSE cases. Based on observations and analysis, training effectiveness can be improved by integrating pedagogical knowledge and focus with each phase of the CSE lifecycle, namely planning, implementation, and feedback. The paper also stated that CSE evaluation necessitates systematic measurements of change ranging from customer experience to organizational change. The research also outlines future research directions for various aspects of expert knowledge development and training evaluation in the context of CSEs.

Moanes H. Tibi (2019) Over the past ten years, cybercrimes have expanded significantly and are now a common occurrence in society. This study sought to determine whether computer science majors at the same college had a higher level of cybercrime awareness than those in other majors by measuring the awareness of cybercrime among teaching students. A sample of 73 Arab students from a teacher training college in the heart of Israel was chosen for this study. For the purpose of gathering information about student awareness of cybercrime, a questionnaire survey was carried out. The study's findings showed that participants' understanding of cybercrime was insufficient, and independent variables including study year, major, and prior computer experience did not produce any statistically significant changes. Additionally, no link between the students' prior computer experience and their propensity to become victims of cybercrimes was discovered. In order to help students avoid becoming victims of cybercrime, it is concluded that higher education institutions should offer training courses on cyberspace security to all students. Finally, suggestions are made for additional investigation.

Moti Zwilling et.al. (2020) Cyber-attacks may pose a threat to information security. As data usage and internet consumption rates continue to rise, cyber awareness has become increasingly important. This study focuses on the relationships between cyber security awareness, knowledge, and behaviour, as well as protection tools, among individuals in general, and in four countries in particular: Israel, Slovenia, Poland, and Turkey. The findings show that while internet users are aware of cyber threats, they only take the most basic and easy-to-implement precautions. The study findings also show that higher levels of cyber knowledge are related to higher levels of cyber awareness, regardless of respondent country or gender discussed.

Moyo (2021) This study examined how well preservice teachers in Cape Town understood cyber security risks during the COVID-19 shift to online learning. It aimed to assess their Cyber Security Awareness (CSA) through a survey of 300 students. Results showed that while basic security measures were used, preservice teachers lacked awareness of advanced cyber threats like data theft and phishing. This gap highlights challenges in protecting personal digital devices used for remote education.

Mudassir Khan and Shameemul Haque (2017) This research investigates the significance of cyber security and ethics in social networking. Cybersecurity has grown in importance in the field of information technology. Securing individual and organizational information has become one of the most difficult challenges in the modern era. People all over the world rely on social media nowadays. Social media is extremely useful in our lives, but it is also being impacted by cybercrime, which is on the rise. Despite the fact that various social media websites provide excellent services, cybercrime is on the rise. Even today, many people are concerned about cyber security. Individuals all over the world are now addicted to social media. Social media has become an integral part of their lives. "How to protect social media from cybercrime" is the main concern. Cyber security is critical for using social media without fear of cybercrime, but it is a difficult task to determine "how to ensure 100% cyber security in the real world." It is also based on cybersecurity techniques used to address cybercrime-related issues. It also focuses on ethics and trends that are altering the face of cyber security.

Neelima Bhatnagar and Michael Pry (2020) This paper describes a study that was designed to gather student perceptions of personal social media risks as well as their knowledge of how to use privacy and security settings in social media applications. A paper-based survey was given to 107 students from 10 classes and 18 different academic majors at a regional campus of a major university in western Pennsylvania. The findings indicate that students are aware of the privacy and security risks associated with the use of social media platforms and value and recommend additional training in this area. This paper investigates a novel concept of a maturity model for social media risk instruction based on various levels of sophistication ranging from basic account settings to advanced concepts of personal brand management. Future research in validating the social media, risk awareness, and countermeasure maturity model is suggested (SMRA-CMM).

Nirmala A.P. and Sravana N (2018) Cyber security is a branch of information technology. Nowadays, one of the most difficult challenges is securing information. Concerning cyber security, the first thing that comes to mind is 'Cyber Crime,' which is on the rise. Many people are still concerned about cyber security. This paper focuses on the various types of cybersecurity challenges. Governments, police, and intelligence agencies are all paying close attention to the issue in the world of computer technology. Various strategies are implemented. The main goal is to educate people around the world and to spread the message that it is no longer safe to navigate the cyber world without security. The techniques used in cyber security were discussed in this paper. Cyber security is concerned with managing future risks as well as responding to current and previous attacks. The report provided a highly standardised and straightforward model for processing risk-management data about critical information infrastructures. Because the world is becoming more interconnected, cyber security is becoming increasingly important.

Osman Sirajeldeen Ahmed et.al. (2021) This study tries to find out how much school teachers are aware of their kids' cybersecurity. Based on a case study of the private schools in the UAE's emirate of Ajman, the teachers' perceptions of their pupils' cybersecurity knowledge were investigated. Ajman's 29 private school teachers were randomly chosen for a survey. A systematic random sample of 172 teachers from the schools in the Emirate of Ajman was chosen as the target population representation after stratified random samples for schools in the Emirate of Ajman were employed. The study's findings show that teachers' awareness of their students' protection and safety has increased in 13 of the variables that were studied while decreasing in 8 other variables. The study also reveals a statistically significant relationship between the variable of specialization and teachers' awareness of their students' cybersecurity, which is primarily driven by the significant differences between the average and the median.

Our digital information is more vital than ever, as evidenced by the literature on cyber safety and security studies. Research indicates that ransomware and phishing are two examples of the cutting-edge tactics that cybercriminals employ to create new and varied cyber threats.

Security against these risks is thought to require the use of technology, such as blockchain and artificial intelligence. Education and training are advised in order to avoid mistakes that could result in breaches because human error is a major worry. A major factor in ensuring businesses and organizations take cybersecurity seriously is the existence of laws and regulations. All in all, the study highlights how important it is to collaborate in order to safeguard our information and be safe online.

Pieter Potgieter (2019) As a result of the lack of regulations, the internet is not a safe place. Users' ignorance of the threats that may confront them in cyberspace can lead to the successful execution of such threats. Before entering the workforce, users should cultivate an awareness culture. As a result, academic institutions should participate in the process of increasing student cyber security awareness (CSA). To communicate effectively on CSA, the user must be familiar with the medium of communication and must engage with it on a regular basis. Students at higher educational institutions report using social media platforms at least once a week, with Facebook and YouTube being the most popular. They also use communication media such as websites to research information. According to the findings of this study, there is a lack of interest among students in participating in available CSA initiatives. It is suggested that academic institutions can help students become more aware by providing them with CSA material on a regular basis. Social media can be used by institutions, platforms (Facebook and YouTube), as well as communication mediums (institutional website and emails) to share CSA information with students.

Prashant Mali et.al. (2018) With the use of the internet, users are progressively becoming themselves subject to security risks. Therefore, questions about users' understanding of these problems and how secure and equipped they are to handle potential circumstances can be raised. This study has offered a survey of current ideas regarding the difficulties posed by cybercrime. It started by examining the definitions of cybercrime and cyberwarfare that were currently in use and discovered two issues that needed to be fixed. First, it was discovered that neither cybercrime nor cyberwarfare had a generally agreed definition. This was problematic because, in the absence of a consensus definition, it has been challenging to talk about the more complicated concerns or even identify when cyberwarfare has taken place. It offers the findings from a research of 325 users to assess their perceptions of security risks, their level of awareness, and their attitudes toward using associated products. The results show that although there appears to be a high level of confidence, with respondents claiming to be aware of the risks and utilizing many of the crucial safeguards, a more detailed reading suggests that there are some areas in which crucial knowledge and comprehension are insufficient. Although a major portion of the problems were frequently severe among new users, there was also egregious ignorance among users who believed they had advanced degrees of online understanding.

Rahman N. A. A. et.al. (2020) report highlights the significance of cybersecurity education in schools, stating that although the Internet has improved people's lives, there are also growing problems associated with its use. Due to the lack of awareness and self-mechanism among Internet users to protect themselves from becoming victims of these activities, cases of cyberbullying, online fraud, racial abuse, pornography, and gambling have significantly grown.

The study found that Internet users still have a low to moderate level of knowledge. One of the most important actions that can be taken is to educate and raise awareness among young children and other Internet users. Children under the age of eight need to be taught how to use the internet safely and how to protect themselves. The study examined the vital components of how contemporary learners are taught about the consequences of engaging in online activity as well as the tactics that stakeholders could employ to advance cyber security education in schools. According to research, it is crucial to protect students through cyber security education so they are aware of any potential threats they may encounter when accessing online communication tools like social media, instructional video games, and the internet.

Rajesh Chandarman and Brett van Niekerk (2017) The study presented in this article aimed to evaluate students' levels of Cyber Safety Awareness at a private tertiary education institution in South Africa. Students were asked to complete a questionnaire that assessed four variables: cybersecurity knowledge, self-perception of cybersecurity skills, actual cybersecurity skills and behaviour, and cybersecurity attitudes. The responses revealed several misalignments, including instances of "cognitive dissonance" between variables, which exposed the students to cyber-attacks. The findings highlight the need for targeted CSA campaigns that address the specific weaknesses of specific user populations.

Ria Hanewald (2008) To increase awareness of the problem and provide information for the discussion that will follow, this review paper covers developments in cyber violence studies from around the world. Most reports of cyber violence, which is a relatively new phenomenon, come from media coverage. Cyber violence and the antidote of cyber safety have become a global concern for governments, educational authorities, teachers, parents and children alike. Despite substantial funding for information dissemination on preventative strategies and the development of electronic responses to hinder perpetrators, the phenomenon of cyber violence has received little attention in the educational research literature. This review paper outlines the status of existing research into cyber violence. Documenting and summarizing the facts on the nature and extent of the issue will inform future debate. It also highlights the need for pre-service and in-service teacher education programs to prepare educators to manage this phenomenon.

Robert Moore (2015) This research paper delves into the topic of cybercrime, including the types, methods, and effects of cybercrime on a network. Furthermore, the study investigates network security in a holistic context, critically reviewing the effect and role of network security in reducing attacks in internet-connected information systems. As a result, all of this has a negative impact on the efficiency of information security of any type that exists and is used in information systems. Since hackers and other criminals in the virtual world are attempting to obtain the most reliable secret information at the lowest possible cost via viruses and other forms of malicious software, the problem of information security - the desire to confuse the attacker: Service information security gives him incorrect information; computer information protection tries to isolate the database as much as possible from outside tampering. In other words, the Internet is a large computer network or a chain of linked computers. Individuals can use this connectivity to connect to countless other computers in order to gather and transmit information, messages, and data. Unfortunately, this connectivity allows criminals to communicate with one another as well as their victims.

Robert “Jake” Bebber (2017) The theoretical framework for assessing a state's prospective cyberpower and efficacy is proposed in this article. It addresses the domestic and systemic factors that affect prospective cyber-power as well as the qualities connected to cyber efficacy. Technical, tactical, operational, and strategic methods are used to convert potential cyberpower into cyber effectiveness. Only when measured in relation to other target states is effectiveness valuable. In order to advance state interests in cyberspace, this paper aimed to better explain and analyze what that entails. In order to do this, scholars are required to put in the effort to assess fundamental ideas like "cyber power" and "cyber effectiveness." Here, a foundation has been provided to place additional study. The example that follows shows how this framework could direct effort in developing hypotheses that investigate different facets of this methodology. Future research questions are then put forth.

Saloni Khurana (2017) The study outlines several cyber-attacks and various security measures that aim to advance the field of study. This study examines the substantial threat that cybercrime now offers to people's lives, as well as some of the numerous security measures being employed in this field and their various flaws. In general, cyber security refers to the methods used to safeguard a user's online environment. The user, their devices, networks, applications, software, etc. are all part of this ecosystem. The major goal is to lower the risk, which includes cyberattacks. The main goal of this study was to describe several cyberattacks and security measures that may be taken to shield devices against assault.

Sarina Yusuf (2018) According to the findings of this study, the prevalence of cyberbullying among Malaysian children is moderate. However, incidents of online harassment occur more frequently than incidents of sexually based cyberbullying. The findings also show that the majority of the children have experienced cyberbullying at least once a year, implying that cyberbullying could become a threat to Malaysian children online over time. Nonetheless, the threat posed by cyberbullying to children has been moderate, implying that the majority of Malaysian children's online safety is currently guaranteed. As a result, this study concludes that mild cyberbullying incidents do occur among Malaysian children, but most of the children are unaware of the implications.

Seemma P.S. et.al. (2018) The study emphasizes the significance of cyber security. Cyber security techniques are generally outlined in published materials and aim to protect a user's or organization's cyber environment. It manages the collection of techniques used to protect networks, programmes, and data from unauthorized access. It refers to a collection of technologies and processes, and it is also known as information technology security. The field is becoming increasingly important as people's reliance on computer systems grows, including smartphones, televisions, and the various tiny devices that comprise the Internet of Things.

Senthilkumar K. and Sathishkumar Easwaramoorthy (2017) The study's objective is to examine college students in Tamil Nadu's awareness of cyber security by concentrating on various online security concerns. Cybercrime has become a significant threat to public safety, personal privacy, and national security in recent years. Everyone needs to be aware of their personal security and safety procedures in order to protect themselves from becoming a victim of cybercrime. College students' knowledge of cyber security has been examined using a well-structured questionnaire survey method. This study was carried out in Tamil Nadu's major cities with a focus on various online security concerns, including spam, viruses, phishing, bogus advertisements, pop-up windows, and other intrusions. This survey examines college students' understanding of security risks and their level of awareness of them, and it offers some solutions.

Shikha Panwar and Dr Mona Purohit (2018) The internet is all around us these days. Additionally, infosec is a crucial aspect of the internet. Web-based services require information security. Every company, institute, and organisation maintains the security of their data and works diligently to keep it that way. The newest technology is regularly taught to security experts by businesses and organizations. Organizations and internet users who use web-based services like social networking, real-time applications, and emails also need information security. Organizations and businesses understand the value of security, but the average user may not be as knowledgeable about the internet or information security. The study will demonstrate the importance of information security for businesses and other internet users, as well as how to protect personal information from hackers and what methods they employ. And the reason why businesses and internet users alike need to be security savvy. And what action should the government take?

Shivani Ghundare et.al. (2020) The necessity for cyber security and some of the effects of cybercrime are discussed in this paper. Cybersecurity is a combination of processes, technologies, and practices. It aims to defend against attacks on programmes, apps, networks, computers, and data. As more systems and applications are being distributed and accessible across insecure networks like the Internet, this need is becoming more and more apparent. Governments, businesses, financial institutions, and millions of daily users now depend heavily on the Internet. Computer networks provide assistance for a wide range of operations whose loss would almost bring these enterprises to their knees. Cybersecurity challenges have thus evolved into national security concerns. The term "cyber security" refers to a broad field that covers the entire underpinning of contemporary civilization and encompasses any intelligence device that can send data to one or more other devices (either through a network or not). Every individual needs to be aware of cyber security, cybercrimes, and the significance of security in relation to online, social media, and other activities where the probability of risk is higher. It results in data loss, data modification, and removal of important information like passwords for bank accounts or email accounts. Also be aware of laws prohibiting cybercrimes, cyber laws, upcoming enforcement measures, and methods for combating crimes.

Shruti Sunil Ajankar and Aditi Rajesh Nimodiya (2021) Cyber security is the safeguarding of computer systems and networks against information disclosure, theft or damage to hardware, software, or electronic data, as well as disruption or misdirection of the services they provide. So, in essence, it is the use of technologies, processes, and controls to safeguard systems, networks, programmes, devices, and data against cyber attacks. Its goal is to reduce the risks of cyber-attacks and protect against unauthorized use of systems, networks, and technologies. The first thing that comes to mind when thinking about cyber security is 'cyber crimes,' which are on the rise. Various governments and businesses are taking numerous steps to combat cybercrime. Aside from various measures, many people are still concerned about cyber security. This paper focuses primarily on some of the techniques and perspectives on transforming cyber security. This study discussed a new posture for cyber security in a networked world, describing how businesses can use organizational structure and governance to improve cybersecurity protections.

Sodha M. S. et al. (2022) This paper describes a cyber-safety and security literacy programme for future teachers. One of the most important and difficult goals of this literacy programme is to raise awareness of and provide basic knowledge about the major cyber safety and security risks in educational and other online environments. This programme primarily focuses on certainly required core competencies (competency in online socialization) and skills for a better cyber etiquette culture, which can be seamlessly integrated into existing teacher education programmes without overburdening teacher trainees.

Sridevi, K. V. (2020) Teaching cyber security to students in schools is crucial for helping them stay safe while using technology. Recently, there has been increased interest in understanding cybersecurity concepts, and institutions have made efforts to introduce these concepts to teachers. Various academic bodies, like NCERT, have developed guidelines and conducted training to create cybersecurity awareness among teachers. In this study, an online survey was conducted to assess the awareness levels of 92 secondary school teachers in Karnataka, India. The findings show that teachers have a medium level of awareness about cyber security, with no significant differences based on gender or stream. However, awareness levels vary with the age of the teachers. This study highlights the need for more research to better understand the importance and implementation of cybersecurity in teaching environments.

Sushma Devi Parmar The paper calls attention to India's experience with cybersecurity as a national security priority. In the age of information, communication, and technology, cybersecurity has evolved into a complex and rapidly evolving security concern (ICT). In fact, as the world's reliance on computers and Internet-based networking grows, there have been more cyberattack events targeting people, organizations, and governments worldwide. As a result, cyber threats are certain to infiltrate every nook and cranny of national economies and infrastructure. ICT is also increasingly being viewed by certain countries as a battlefield where strategic wars can be fought as well as a strategic asset to be used for the reasons of national security. In order to enhance the analysis and assess the importance of cybersecurity in the current security dispute, this article analyzes cybersecurity from the viewpoint of India.

Teresa M. Lester (2018) The research highlights there is a need to recheck the levels of understanding and difference in perspectives about cyber safety and how that knowledge is applied and used as technology changes constantly. It is time to educate teachers and parents on how they can teach themselves and stay on top of changing technology trends and to share the knowledge they have learned in the process. The purpose of this mixed-methods investigation was to determine how teachers and parents understood and educated themselves on cyber safety. This research explored how teachers and parents found and used resources available to stay informed of the constant threats and changes for students while online. Using an online mixed-methods survey and interviews, the researcher sought to determine, compare, and examine the levels of understanding and perspectives of teachers and parents on cyber safety issues and training. This study was used to determine if there was a need for more readily available training on the issues concerning cyber safety for teachers/parents to ensure the safety of students/children in K-12 schools and communities.

Tomczyk, Ł. (2020) The goal of the research was to assess the level of Digital Literacy (DL) among teachers, focusing on six key areas: ICT ergonomics, assessing information credibility, secure online communication, maintaining digital anonymity, safe logging-in, and intellectual property. Conducted in Poland in 2017/2018 with 701 primary school teachers, the study used a knowledge and competence test to measure DL. Findings revealed that DL is varied, with teachers showing the least knowledge in intellectual property law and the most in ergonomics. Gender did not affect DL levels, and the Dunning-Kruger effect was evident in teachers' self-evaluation of digital safety skills. The study highlights DL as a critical protective factor in digital safety for schools, making it essential to diagnose and enhance DL among teachers.

Tosun, N., & Akcay, H. (2022) This study aimed to assess awareness and experiences of cyberbullying among administrators and teachers in preschool education institutions in Edirne, Turkey. The objectives included determining levels of awareness about cyberbullying, identifying instances of cyberbullying among educators, and examining strategies employed to combat cyberbullying. The study involved 15 preschools, both public and private, with participants from the Ministry of National Education. Data collection utilized the Cyberbullying Scale for University Students by Tanrikulu and Erdur-Baker (2019), along with survey and interview forms designed by the researchers. Findings indicated that cyberbullying levels among administrators and teachers were lower than cyber victimization rates. Younger educators were more likely to engage in cyberbullying compared to older colleagues, and those unfamiliar with cyberbullying were more prone to perpetrating it. Participants primarily learned about cyberbullying through social media and advocated for seminars and family education to combat this issue. These insights underscore the need for targeted interventions to enhance awareness and prevention strategies in preschool settings.

Urmila Goel (2014) The goal of the current study is to ascertain the level of cybercrime awareness among B.Ed. Teacher candidates. A sample of 120 B.Ed. Students from the Sonipat area were chosen for this purpose. The information was gathered using the Dr. S. Rajasekar-created Cyber Crime Awareness Scale (CCAS-RS). According to the study, there is no discernible difference between boys and girls in terms of their awareness of cybercrime. There is no discernible difference between rural boys and females in terms of awareness of cybercrime. Urban boys and girls, science and art boys and science and art girls have quite different perspectives on cybercrime awareness. The findings indicate that although gender, whether male or female, does not significantly influence awareness of cybercrime, area, whether rural or urban and stream, whether science or art, may considerably influence awareness.

Wejdan Aljohani and Nazar Elfadil (2020) The authors of this study created a questionnaire instrument to assess the students at Fahad Bin Sultan University (FBSU) current level of cyber security awareness (CSA). The questionnaire was created to achieve the aims and objectives of this research project. This paper's primary objective was to assess the degree of cyber security knowledge among FBSU students. Additionally, the cyber security students' awareness level questionnaire was modified from a few previous questionnaires that dealt with cyber security awareness. 212 pupils in all took part in the poll. According to the study's findings, there has been no difference in the knowledge levels of male and female pupils when it comes to cyber security. The findings of the survey tool also show that the module has been successful in gauging students' knowledge.

Yang J.C. et.al. (2018) According to the findings of this study, there is a lack of interest among students in participating in available Cyber Security Awareness (CSA) initiatives. It is suggested that academic institutions can help students become more aware by providing them with CSA material regularly. Social media can be used by institutions, platforms (Facebook and YouTube), as well as communication mediums (institutional websites and newsletters). e-mails) to share CSA information with students. This research explains the roles of the primary trainers and the characteristics of the secondary trainers in the Teacher Professional Development cascade model. It was discovered that secondary trainers require knowledge of the training domain, experience from previous related workshops, and participation in sessions led by primary trainers. Other important characteristics of secondary trainers include content ownership, feedback from Primary Trainers, and time management. The primary trainers are involved in the selection of the secondary trainers and provide them with ongoing feedback. Further research will be conducted to determine how the findings from these secondary trainers can be applied in cascaded training programmes involving more than two levels, multiple sessions per secondary trainer, and the use of technology to train participants.

Yogesh Shelokar and Prof S. Vyawahare (2019) This project uses survey reports from parents of students aged 17 and under to assess the level of cyber security parental awareness to protect their children. The distribution of positions was used to interpret a quantitative data analysis performed with Project software. During the analysis method, a combination of general profiling of respondents and descriptive statistics were used. Any findings from this project would necessitate a greater focus on the proposed Cyber Parenting Model in order to identify the factors that influence Internet safety at home. Early exposure to parental awareness would aid in increasing parental knowledge of cyber security.

Yuxi Wu et.al. This study examines prior work in social cybersecurity and organizes it according to its relevance to four Standard and poor (S&P) relevant social behaviours negotiating access to shared resources, shared and social authentication, managing self-presentation, and influencing others' S&P behaviours. It further divides these domains into four social distance scales-intimate, personal, social, and public—demonstrating how desired access control policies, authentication methods, and privacy and sharing preferences vary across these social scales. The researchers examined the current work landscape through the lens of Ackerman's social-technical gap in social computing systems, discovering that while social behaviours clearly influence S&P preferences and needs, existing S&P systems are designed with little understanding of these behaviours. Because of this mismatch, users must choose between implementing their ideal S&P policies and reducing social friction. To address this misalignment, we propose a social cybersecurity research agenda that better aligns S&P goals with social needs, preferences, and behaviours.

Yılmaz Vural et.al. (2016) Critical company and individual security safeguards must be implemented in order to minimize the impact of such cyber attacks on the national level. One of the first things that needs to be done is the establishment of enterprise and personal information security, which forms the stages of establishing national information security at the highest level and the development of a national security strategy. This paper first identifies the critical national information systems before describing personal and corporate information security, which are crucial steps in securing the national information systems. The following section discusses the required security checks as well as the value of knowledge and awareness. Finally, assessments of the nation's information security have been made, and recommendations have been made.

2.3 Conclusion

The Cyber Safety and Security Awareness Package for Teachers has been found to be successful in improving teachers' knowledge of cyber safety and security problems. Teachers reported feeling more confident about securely navigating the digital world and imparting these ideas to students, which resulted in positive behavioral changes and the adoption of safer online habits. The contents in the package, which were both comprehensive and flexible, were well-received and made it easier to include cyber safety into the curriculum. The study's conclusions highlight how important it is for educational policymakers to give priority to cyber safety training for educators and to offer continuing support and updates in order to stay up to date with the constantly changing landscape of cyber threats. Additionally, the study suggests that schools should promote a culture of cybersecurity awareness and resilience.

CHAPTER 3:METHODOLOGY

3.1 Introduction

The research paradigm's methodology is an essential component. The rationale and flow of the methodical techniques used to collect data on a research question are explained by the methodology. It describes the underlying presumptions, boundaries found, and strategies for managing or minimizing them. This chapter explains the many approaches that were employed to collect and analyze data that were pertinent to the study. The study's location, research design, sample size and sampling strategy, data kinds, data gathering methods, and data management are only a few of the topics covered by the techniques.

Research is a methodical approach to the study of certain phenomena. The philosophical foundation for education research is provided by the research paradigm. Because these practices and discourses are embedded in national education systems and have a long history of development, education research focuses on how they relate to the idea and comprehension of education. Educational study encompasses the nature, structure, and evolution of regional, national, and global education systems. In the area of educational technology research, which is a subset of educational research, this is particularly clear.

The methodology of the study refers to the overall plan created and adhered to in order to address research questions and assess hypotheses in the field of educational research. The entire study roadmap for the national level is covered in this chapter, along with the technique that involves quantitative research and data collection to ascertain teachers' knowledge levels of cyber safety and security.

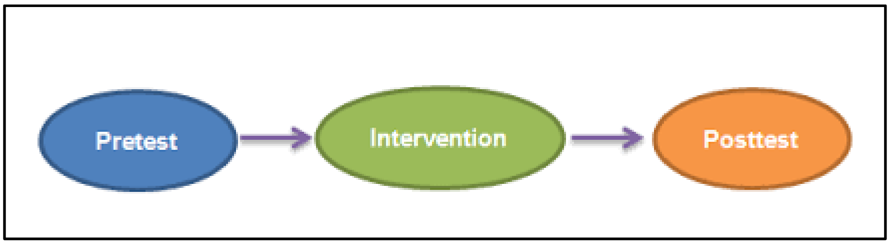
Research consistently shows that teachers with a variety of backgrounds who often use computers and the internet are not well-informed about cybersecurity risks. Moreover, there is no standard procedure for evaluating the views and inclinations of online users about cybersecurity safety measures. Due to the increased reliance on digital platforms and technologies for instruction, cyberattacks are becoming a greater risk for educational institutions, students, and teachers. Participants in the teaching-learning process need to be properly trained since ignorance might result in risky online behaviours that enhance exposure to cyberattacks.

The project's objectives are to measure teachers' understanding of cyber safety and security, analyze and identify dimensions, and produce an intervention package. Thus, ***"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers"*** is how the problem statement is phrased.

3.2 Research Design

The research design was based on the need to develop a Cyber Safety and Security Awareness Scale and a Cyber Safety and Security Intervention Package. The research aims to identify various dimensions involved in cyber safety and security awareness and identify the level of awareness across those dimensions in the selected sample. Methods used in Assessing teachers' current knowledge and practices before the training (Pre-test) Providing the cyber safety and security awareness package to the selected teachers (Intervention) and Re-assessing their knowledge and practices after the training to measure any improvements (Post-test). Data was collected using surveys to gather information from teachers. Finally, Compare the pre-test and post-test results to determine if the training had a positive impact.

This study will utilize the pretest,intervention and post-test.



3.2.1 Design of the Study

The study investigated teachers' awareness of cyber safety and security at the national level using the survey method, a quantitative research approach that maximizes descriptive and inferential statistics.

In the social sciences, survey research is a popular method because it enables researchers to gather information on a wide range of subjects pertaining to the thoughts, feelings, and behaviours of individuals or groups. According to Buchanan and Hvizdak (2009), the objectives of survey research include characterizing a population, defining group characteristics, describing traits and attributes of interest for the study, elucidating a phenomenon, and explaining the relationship between variables. A lot of research in education uses online questionnaires (Roberts & Allen, 2015). The use of online surveys is expanding. Perhaps due to their ease of use, affordability, and simplicity, online surveys are growing in popularity (Andrade, 2020). An internet survey and a random-digit-dial phone survey were the two most often used social science techniques in the past few decades to collect extensive recreation data. Cyber security awareness training can be defined as the technical approach to create awareness among all of them about the importance of data privacy, people's identities, and other assets which are often hacked by internet criminals.

The design of the research was based on the need to develop a Cyber Safety and Security Awareness Scale and a Cyber Safety and Security Intervention Package. The research aims to identify various dimensions involved in cyber safety and security awareness and identify the level of awareness across those dimensions in the selected sample. The developed Cyber Safety And Security Intervention Package was implemented in the selected sample and a post-assessment was conducted to study the impact of the intervention package. The post-assessment scores were analyzed to study the objectives of the research. Further feedback collected from the sample was analyzed in order to comprehend future training. The Cyber Safety And Security Intervention Package consists of:

1. Online Training for the Selected Teachers
2. Self Learning Package
3. Advanced on Cybersecurity Training for Teachers (ACTT)

4. Post Assessment
5. Feedback

This study aimed to evaluate the effectiveness of an online training designed to enhance cyber safety and security awareness among teachers within educational settings. The three-day State Resource Group training on Cyber Safety and Security provided an in-depth understanding of various dimensions of cyber safety and security through eight sessions. These sessions were based on five key dimensions: technical, physical-psychological, socio-ethical, legal and concept of cyber safety. The technical aspect comprised four sessions: Device Safety and Security, Browser and Email Security, Digital Financial Security, and Social Media and Safety, Cyber Scams, and Frauds. These sessions covered essential practices to protect devices from malware and unauthorized access, safeguard online browsing and email communication, implement robust financial security measures, and mitigate risks associated with social media usage and common cyber scams. The session on Psychological Issues in the Context of Cyber Safety and Security explored the mental and emotional impacts of cyber threats, such as cyberbullying, online harassment, and identity theft, emphasizing the importance of mental well-being in the digital age. The Social and Ethical Aspects of Cyber Security session examined the broader implications of cyber activities on society, covering topics such as digital citizenship, ethical hacking, and social responsibilities. Lastly, the session on Legal Frameworks for Cybersecurity provided an overview of legal measures in place to combat cybercrime, discussing relevant laws, regulations, and the role of law enforcement agencies.

Each session was conducted by experts in the respective fields, ensuring that participants received high-quality, authoritative information. The sessions lasted approximately 1.5 hours each, where experts presented their content through detailed PowerPoint presentations and engaged with participants by answering questions at the end of each session. To maintain a coherent flow and enhance the learning experience, the sessions were strategically arranged, with practical sessions following the expert presentations on the first and second day. These practical sessions were designed to reinforce the theoretical knowledge gained during the expert sessions. Participants were divided into breakout rooms based on their states/ UTs, Autonomous Organizations, and various constituents of NCERT, facilitating focused discussions and collaborative learning. They were given specific assignments related to the topics covered in the sessions, required to discuss these assignments with their team members, formulate collective responses, and document their findings in a shared Google document or slide. This collaborative approach not only reinforced the learning but also fostered teamwork and communication among participants from different regions and organizations. The three-day State Resource Group training on Cyber Safety and Security was a comprehensive program that addressed multiple dimensions of cybersecurity. By combining expert-led sessions with practical, hands-on activities, the training provided participants with the knowledge and skills needed to navigate the complex landscape of cyber threats. The structured flow of sessions and the collaborative assignments ensured that participants could effectively absorb and apply the information, contributing to a safer and more secure digital environment.

The methodology employed includes a pre-test, intervention, and post-test approach for each session to assess participants' knowledge and skills before and after the intervention. For each session, participants first completed a pre-test to assess their baseline knowledge and understanding of the session's topic. The interventions, delivered by experts in their respective fields, provided in-depth insights and practical strategies on various aspects of cyber safety. Following each intervention, a post-test was administered to measure the knowledge gained and the effectiveness of the session. The interventions included presentations and discussions led by specialists, focusing on essential practices and strategies in these areas. The post-tests assessed improvements in participants' knowledge and their ability to apply the concepts discussed during the sessions. The post-test was assessed through multiple-choice questions.

3.2.2 Variables of the Study

Variables are the factors involved in addressing the research problem, which leads to the closure of the research gap. These attributes ought to impact one another. The current study seeks to investigate variables like teachers' level of awareness of cyber safety and security. Hence, the following independent and dependent variables were identified for the investigation of the study:

Variables are the factors involved in addressing the research problem, which leads to the closure of the research gap. These attributes ought to impact one another. The current study investigates teachers' levels of awareness of cyber safety and security. Hence, the following independent and dependent variables were identified for the investigation of the study:

- **Independent Variable**

Variables that have undergone manipulation are considered independent variables. A variable that modifies to observe how it impacts another component is known as an independent variable. So, in this study, Gender is considered as an independent variable.

- **Dependent Variable**

A dependent variable is the measured or observed variable. This study tries to find out how the dependent variable is affected by the independent variable. In this study, the awareness on cyber safety and security is considered as the dependent variable and the study intends how the awareness varies across the selected independent variables. By observing the dependent variable, the effect of the independent variable can be measured. It was tested whether the independent variable would have an effect on the dependent variables i.e., 'Awareness package' on Cyber Safety and Security for Teachers.

3.2.3 Hypothesis of the Study

To undertake a meaningful analysis, the following hypotheses were proposed.

H_1: There is no significant difference in the pre-test and post-test scores on cyber safety and security awareness between male and female teachers.

H_2: There is no significant difference in the pre-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security

- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_3: There is no significant difference in the post-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_4: There is no significant difference between male and female teachers in their pre-test scores with regard to the Concept of Cyber Safety and Security domain.

H_5: There is no significant difference between male and female teachers in their pre-test scores with regard to the Device Safety and Security domain.

H_6: There is no significant difference between male and female teachers in their pre-test scores with regard to Browser, Email Security and Digital Financial Security domains.

H_7: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social Media and Safety domain.

H_8: There is no significant difference between male and female teachers in their pre-test scores with regard to the Cyber Scams and Frauds domain.

H_9: There is no significant difference between male and female teachers in their pre-test scores with regard to the physical and psychological domains.

H_{10}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{11}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Legal Frameworks for the Cybersecurity domain.

H_{12}: There is no significant difference between male and female teachers in their post-test scores with regard to the Concept of Cyber Safety and Security domain.

H_{13}: There is no significant difference between male and female teachers in their post-test scores with regard to the Device Safety and Security domain.

H_{14}: There is no significant difference between male and female teachers in their post-test scores with regard to the Browser, Email Security and Digital Financial Security domain.

H_{15}: There is no significant difference between male and female teachers in their post-test scores with regard to the social media and safety domain.

H_{16}: There is no significant difference between male and female teachers in their post-test scores with regard to the cyber scams and frauds domain.

H_{17}: There is no significant difference between male and female teachers in their post-test scores with regard to the Psychological Issues In the context of Cyber Safety and Security domain.

H_{18}: There is no significant difference between male and female teachers in their post-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{19}: There is no significant difference between male and female teachers in their post-test scores with regard to the legal framework for the cybersecurity domain.

3.3 Sampling Strategy

3.3.1 Population of the Study

The population of the present study is all the Teachers, Teacher Educators, Administrators and educational stakeholders from various States/ UTs and Autonomous Organizations like CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS. The target group also includes Teachers, Administrators and Faculty of various constituent units of NCERT like DMS, RIEs, NIE, and PSSCIVE from all 28 Indian States and 8 Union Territories. There are about 16 million teachers in the 2022-23 session (MoE, 2022) and all of them were considered as the population of the present study.

3.3.2 Sampling Technique

Sampling is the process of selecting a small group from a large population to act as that population's true representative. Sampling is the process of selecting a subset from the entire population or a predetermined sampling frame. Sampling can be used to draw conclusions about a community or to draw broad conclusions about current theories. Essentially, the selection of the sample technique determines this. Generally speaking, there are two categories of sampling techniques: Random sampling or probability and Non-random or non-probability sampling (Taherdoost, 2016). In the context of a large and geographically dispersed population, a more complex technique known as multistage sampling is employed. Multistage sampling is a complex form of cluster sampling in which the selection of samples is carried out in multiple stages (Cochran, 1977). At each stage, the population is divided into clusters or groups, and a random sample of these clusters is selected. Within each selected cluster, further sampling is done to select smaller units, and this process is repeated as necessary.

Given the vast geographical size and diversity of the population, the documented report utilized a four-phase sampling process to create the final sample for the investigation. In the first phase, the sample encompassed the entire population across all 28 states and 8 Union Territories (UTs). In the second phase, the sample included the entire population across all Autonomous organizations/ NCERT. The third phase focused on categorizing data by school type, covering CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS and DMS including their entire teacher populations. Only teachers who were using the Internet were included in the final sample for this study.

The sample was collected in two phases:

Phase 1: Selection of States and Union Territories

The first phase involved choosing every single person living in all 28 states and 8 Union Territories (UTs) in India, all 36 entities were taken. Ensuring geographic coverage and variety, this phase captured the whole range of regional variances and traits.

Table 3.1

States/UTs	Selected	Remarks
36	36	Entire Population was taken

Phase 2: Selection of School Boards/Autonomous organizations/ NCERT

In the second phase, every teacher in every state and UT across all approved school boards and Autonomous organizations/ NCERT was included in the sample. This stage was essential to creating a thorough depiction of the educational environment by incorporating the various curricula and educational systems.

Next, selecting the entire population of teachers and teacher educators from all types of schools, such as government, private, and aided, which are affiliated to the state board and Central Board of Secondary Education (CBSE).

Table 3.2

School Type	Selected	Remarks
Government & Aided Private	CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS /RIE/NIE/DMS/PSSCIVE	Entire Population was taken

3.3.3 Sample Size

In order to conduct the research, purposive sampling was done. Hence, all the States/UTs and autonomous organizations were requested to select and depute Teachers, Teacher Educators, Administrators and educational stakeholders. 20 participants were deputed from each state/UTs and 5 participants were deputed from each autonomous organization. The sample coverage was 470 teachers teaching in any school, whether Government, Private, or Aided school, from all 36 States / Union Territories.

Table 3.3 Gender-wise sample distribution

S. No.	Gender	Sample
1	Male	311
2	Female	159

3.3.4 Access and Permission

The project has been approved by the Central Institute of Educational Technology, NCERT, New Delhi. Access and permission were obtained from school heads and heads of Autonomous Organizations. The consent of respondents was obtained through consent guidelines via the online survey. This research aimed to gather valuable insights into teachers' awareness and practices regarding online safety.

3.4 Research Tool

One of the most common types of assessments is a multiple-choice test. When presented with a question in a traditional multiple-choice test, a candidate must evaluate each option and select the most appropriate (Ng,2009). The study used an online survey method with a quantitative design; therefore, creating a tool to collect the required data was unavoidable. The research team examined a wide range of relevant literature in order to construct the tool "Effectiveness of Cyber Safety and Security Awareness Package for Teachers," including country reports, peer-reviewed research articles from India and abroad, cyber safety and security guidelines for teachers from various national and international agencies, policy documents from India and abroad, expert opinions, etc. Dimensions were determined, and the multiple choice scale was developed. The scale has five dimensions: Technical, Legal, Socio-ethical, Physical-Psychological and concept of cyber safety. Each session contributed 10 questions to the assessment except the technical (40 questions). A comprehensive assessment was administered at the end of the training, consisting of 80 questions in total.

3.4.1 Identification of Dimensions

A Multiple choice scale with four dimensions on cyber safety and security was constructed, validated, and reliability was achieved by going through pilot testing. A Google form was created in English language and translated into Hindi also for the collection of data and the link was shared with all the 36 states and UTs of India for the purpose of collecting data from teachers for the study. Five dimensions of the Multiple choice scale are shown below:

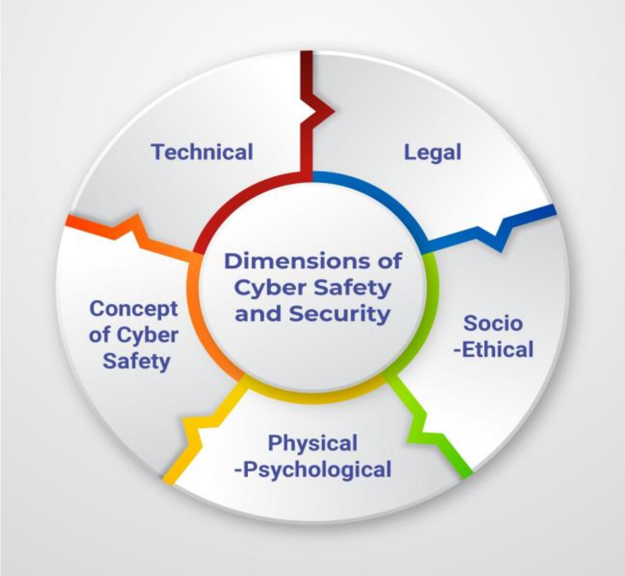


Figure 1: Dimension coverage

The awareness scale consists of five dimensions and the concept of cyber safety and security information domain is also included with 80 items with 4 responses.

3.4.2 Identification of Parameters and Attributes

Selection and Compilation of Items. Initially, a Focused Group Discussion was organized on the following questions:

1. Due to the use of digital devices, what changes do you see in lifestyle and behavioral patterns?
2. Who do you think is more appropriate to approach when you come across cyber-related problems? Teacher, Counselor? Psychologist and Why?
3. How will you handle it if you and your friends are cyberbullied?
4. How do you protect your digital device? Explain.
5. What precautions do you take when you access public WIFI?
6. What information will you share publicly or on social media platforms?

In this Focused Group Discussion, five dimensions of the multiple-choice questionnaire were finalized. 120 items were developed through a rigorous review of literature available on different websites, previous studies were also considered for selecting items. After the discussion with experts, 80 items were found suitable.

A 3days extensive online training programme on cyber safety and security awareness was designed based on the background research and review of the literature. The participants received the cyber safety and security awareness training programme that covers various aspects of cyber safety and security, including technical, legal, socio-ethical, physical-psychological and concept of cyber safety. The training delivered in 3 days used various methods, such as lectures, case studies, quizzes, videos and interactive activities. The online training covered the dimensions of cyber safety and security selected for the study:

1. **Technical Dimension:**

   The technical component of the training included information on how to use and teach safe online tools and technologies in the classroom, orientation on different types of cyber threats such as malware, phishing, ransomware, and social engineering attacks and the best practices for creating and managing strong passwords. It also discussed configuring privacy and security settings on devices and social media platforms. It was also discussed how virtual private networks (VPNs) can be used for secure browsing and remote access.

2. **Legal Dimension:**

   The legal component of the training included a guide to identify and report cybercrimes and online harassment. It discussed the implications of cyberbullying and cyber harassment on individuals and society. Further, it explained the importance of respecting intellectual property rights and avoiding online piracy.

3. **Socio-Ethical Dimension:**

   The ethical component of the training covered a discussion on appropriate ethical behavior online, including honesty, respect, and responsibility in the educational system. The trainer focussed on developing critical thinking skills to evaluate online information and the relevance of promoting responsible digital citizenship behavior. The participants were taught about online privacy, protecting personal information and Identifying unethical online behavior such as cyberbullying, trolling, and cyberstalking.

4. **Physical-Psychological Dimension:**

   The psychological dimension focused on understanding cyberspace on human behavior, cognition and its impact on well-being. Participants were oriented on promoting positive online behavior and respectful online communication among students. Providing support to victims of online harassment or abuse in the classrooms and understanding the reporting mechanism. Further emphasis was given to promoting good digital hygiene habits and encouraging students to balance online and offline activities.

The single-group pretest-posttest research design was followed for this study. Post the cyber safety and security awareness training, the group was administered an assessment to assess their level of knowledge and awareness of cyber safety and security in all five dimensions.

3.4.3 Development of the Items

As cited above there was a Multiple choice scale used in this study. A brief description of the Multiple choice scale' development is presented in the following heads- Scale for teachers:

Structure of Multiple choice scale- Blue-print of teachers' Multiple choice scale

Table 3.5

Purpose of the Scale	A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers	
Nature of the Scale	Structured, Close Ended	
Sessions	Concept, need and scope Device Safety and Security Browser, Email Security and Digital Financial Security Social Media and Safety Cyber Scams and Frauds Psychological issues Social and ethical aspects Legal frameworks	
Dimensions	Technical	40
	Legal	10

	Socio-ethical	10
	Physical -Psychological	10
	Concept of Cyber Safety	10
Total number of items		80

3.4.4 Development of the Research Tool:

One of the objectives of the research was to develop a research tool to measure the level of cyber safety and security awareness among teachers, teacher educators and school administrators. In the research process, a workshop was conducted to gather expert input, which was then complemented by a thorough analysis and review of existing literature. This combined approach was utilized to identify and define the primary dimensions for the development of the measurement scale. pon identifying the dimensions, parameters and sub-parameters were defined under each dimension. Further, for tool development, individual items were designed under each dimension covering all the parameters. The research tool developed by CIET-NCERT is termed “The Cyber Safety And Security Awareness Scale”.

A series of workshops were also conducted at CIET-NCERT to review the scale from external experts.

Workshop 1: To review the Tool Developed

A Three days workshop was conducted to review the questionnaire developed with the following objectives:

- To review the cyber safety and security awareness research tools developed for students, teachers, and administrators.
- To finalize the cyber safety and security awareness research tools developed for students, teachers, and administrators.

The workshop was conducted in the blended mode where resource persons were given an option to join the workshop in face-to-face mode from CIET-NCERT whereas outstation resource persons from ISEA-CDAC had an option to join the workshop online and review the parameters and items developed to assess the level of cyber safety awareness among various stakeholders. At the end of this workshop, all the items of the tool were reviewed and the tool was finalized. The finalized research tool developed which is termed as “Cyber Safety And Security Awareness Scale” consists of 80 items, each part consisting of 5 dimensions namely, technical aspects, legal aspects, social-ethical aspects and physical-psychological and concepts of cyber safety aspects. These 5 dimensions cover 16 parameters and 25 sub-parameters. The developed questionnaire is attached as Annexure I.

3.4.5 Pilot of Research Tool

A feasibility study, sometimes called a pilot study, is a small-scale investigation carried out before a more extensive, full-scale investigation. It serves as a trial run to evaluate the viability, usefulness, and efficacy of the techniques and protocols intended for the primary study. A pilot study was done on a small sample of teachers. A sample of 47 teachers was chosen, and the research tool was administered to them to establish the reliability, viability, usefulness, and efficacy of the research tool.

3.4.6 Validity and Reliability

Validation of Tool: The validity and reliability of the scales employed in research are critical aspects that allow the research to provide useful results. For this reason, it is important to understand how researchers appropriately assess the scales' reliability and validity (Surucu & Maslakci, 2020). A research study may comprise only part of the methodological subspace's elements, which include scientific standards, procedures, and principles. Examples of these elements are validity systems. This subspace is utilized in substantive research to establish knowledge claims and comprises information derived from methodological research (Lund, 2022).

The literature synthesis produced themes and codes for item development in scale based on worldwide and Indian research papers, reports, and policy guidelines, as well as the identified research deficit. The expert members structured the questions and items on the background variables and dimensions of the scale using the themes and codes. The scale contains Four dimensions: psychological, physical, legal, socio-ethical, and technical. Individual Items were developed using the dimensions. The developed questions on the background variables and items under each dimension were then examined for face validity and content validity by the national-level experts. Based on their validity examination, some items were removed, and a few were added.

- **Face Validity:** Face validity was checked by the research team members first, and then by the Program Coordinator, 80 questions and 5 dimensions were finalized.
- **Content Validity**. The rating scale was validated by 7 experts in the field. Later, the panel of experts was formed based on expertise in psychology, sociology, law, and educational technology; a minimum of five years of experience in concerned fields was required. Three professors and four assistant professors constituted the panel of experts.

The experts' suggestions regarding objectivity, and suitability of items were taken into consideration. Language difficulty was removed by replacing difficult words with easy ones. In the final rating scale out of 120 items, 80 items were selected and reframed according to the need of the study and the rest were removed. All the suggestions given by experts were incorporated into the final tool. It is only after the validation; that the tool was administered to the sample.

To determine the flaws and limitations and to achieve reliability and validity of the rating scale, pilot testing was done on a small sample of 47 teachers. It enables us to refine the instrument and make necessary improvements before the final implementation. A pilot test was conducted on 47 teachers to ensure the accuracy of items and whether it addressed research questions or not.

Reliability of Research Tool:

Reliability refers to the consistency and stability of a measurement over repeated administrations or observations. A reliability score close to 1.0 indicates a high level of consistency, meaning that the measurement is highly dependable and yields similar results under consistent conditions. The statistical analysis was conducted using version 28.0 of the Statistical Package for the Social Sciences (SPSS). Cronbach's alpha was used to determine the CSSAS quality score's internal consistency. A reliability score of 0.8 was derived from statistical analyses, indicating that the measurement instrument has demonstrated exceptional reliability in the context of the research study. In research, a reliability score of 0.8 typically indicates a very high level of reliability of the tool. It also suggests that the measurement instrument or tool used in the study demonstrates an extremely high level of consistency and stability. This high-reliability score implies that the measurement is highly trustworthy and can be relied upon to produce consistent and accurate results across multiple administrations or observations.

3.4.7 Finalization of Questionnaire:

After the pilot study, a few more modifications were made to the multiple choice questionnaire before the final administration of the teachers. Here irrelevant and invalid items were removed, and at the end, 80 items were left in the final multiple-choice scale.

3.4.8 Translation of Research Tool:

Translating a research tool is critical for guaranteeing the inclusion, precision, and validity of research. Translating a research tool makes it accessible to individuals who do not speak the original language. Translation of research tools into other languages ensures that teachers who do not know the original language have equal access to participate in the study; it may improve sample representativeness and generalizability.

The translation process is extensive and detailed, requiring knowledge of the subject idea, conversion, and presentation of complicated concepts in their simplest form. The population covers teachers, teacher educators and school administrators from all 28 Indian States and 8 Union Territories, and the sample was selected from that, so the translation of the awareness scale in the mother tongue was required.

The current study used a quantitative research design, which is empirical in nature i.e., it focuses on numbers and statistics and is critical for revealing the educational landscape. It is effective for educators, policymakers, and researchers alike, providing crucial insights to inspire evidence-based policies and enhance learning outcomes. The study includes all 28 States and 8 Union territories in India. An online survey method was used to collect data from multiple schools, including diversity in population, school settings, languages, etc. A descriptive survey was done using Google Forms among teachers to find out their awareness of cyber safety and security based on different dimensions. Getting accurate details on an existing situation is the aim of a descriptive survey study in order to decide what should happen next (Good, 1972). An Online-based survey was used to collect the data. This was due to covering samples of all 28 Indian States and 8 Union Territories. Permission from the school authorities/ heads was obtained, and consent was also obtained from the teachers for the data collection.

Time allocation was maintained for each step of the empirical investigation of this study, including project conception, literature review, tool construction, validation, pilot study, reliability attainment, primary data collection, data analysis, and report writing.

The online tool was administered in English and bilingual mode, and a Google form link of the research tool was shared with each of the 28 States and 8 Union Territories in India for fifteen days.

3.5 Data Collection:

The next step after defining the sample and instrumentation is data collection. The Google form multiple choice questionnaire scale was directly sent to the states and UTs, which was further shared with the sample teachers. The consent of the teachers, teacher educator and school administrator was taken.

3.6 Data Analysis

The quantitative data was analyzed under descriptive and inferential parameters. The items which are in the scale have multiple-choice-based connotations based on the connotations with respect to cyber safety and security. Each item has 4 responses. For scoring purposes, each correct response is awarded 1 point, while each incorrect response receives 0 points respectively. The results were presented in tables and figures. The quantitative data was analyzed under descriptive and inferential parameters. Ms-Excel was used for Descriptive analysis, and SPSS Software for inferential analysis; independent sample t-tests were used. The result was presented in tables and figures.

3.6.1 Statistical Analysis for Quantitative Data

Statistical analysis is an essential component of quantitative research (Kee et al., 2013). Quantitative data is usually associated with numbers, and Quantitative research has the advantage of establishing a sequence of processes that allow for the standardized investigation of phenomena, thus significantly reducing the researcher's bias (Suárez et al., 2017). A popular approach for formulating and addressing quantitative research questions is to identify a gap in the current literature and conduct a study to fill it (Jamieson et al., 2023).

For the statistical analysis, data was exported to an Excel file and was cleaned. After this, the collected data which were in alpha-numeric format were coded to numerics, so as to make the analysis easier. The score of the CSSA tool was calculated dimension-wise as well as in total. The cleaned and coded data was then exported into SPSS (Version 27) for further analysis. The details of the analysis carried out along with the findings and discussion are presented in the following chapter.

3.7 Limitations of Study

This nationwide quantitative study has its own limitations. They are limited with gender, Coverage of dimensions, Research method and coverage of languages in tools.

- **Gender:** The study is limited to examining the effectiveness of the cyber safety and security awareness package for teachers with a specific focus on gender. It explores how male and female teachers perceive and benefit from the awareness package, analyzing any differences in their responses and outcomes.
- **Dimensions of Cyber Safety and Security:** The study concentrated only on four dimensions of cyber safety and security that are pertinent to teachers including Physical-Psychological, Legal, Socio-ethical and Technical. This boundary guarantees a targeted analysis of the most important cyber safety and security concerns that affect the intended sample.
- **Research Method:** The study adopted online surveys through Google Forms and quantitative analysis.
- **Language coverage:** The tool of the study was prepared in English and Hindi.

The results and interpretation along with its discussion will be presented in the next chapter.

3.8 Conclusion

The methodology of this study was designed to effectively evaluate the Cyber Safety and Security Awareness Package for teachers. An online survey was used for data collection, featuring multiple-choice questions to gather detailed data efficiently from a large number of participants. This approach was suitable for the descriptive nature of the research, allowing for clear and measurable results. Multiple-choice scales within the survey helped measure teachers' knowledge, confidence, and behavior changes before and after the training. The online format made it easy for teachers to participate, regardless of their location. Statistical analysis showed significant improvements in teachers' understanding and practices related to cyber safety and security. Overall, the methodology successfully captured the necessary data to conclude that the awareness package was effective in enhancing teachers' cyber safety and security awareness.

CHAPTER 4: RESULTS AND INTERPRETATION

4.1 Introduction

Data analysis is the systematic procedure of applying logical and statistical methods for describing, illustrating, condensing and assessing the research data. According to Creswell (2002), qualitative research is a strategy for data collection, analysis, and report writing that is distinct from the conventional, quantitative approaches. Quantitative research is the process of gathering, analyzing, interpreting, and producing study results.

4.2 Data Analysis and Interpretation

Analyzing and interpreting data entails systematically going over gathered information to find trends, connections, and revelations that help with decision-making. This procedure entails cleaning and arranging the data, analyzing it using statistical or computational techniques, and producing a meaningful summary of the results. Interpretation is more than just summarizing the findings; it also entails placing the data in the larger context of the study question or issue, coming to conclusions, and drawing conclusions from the analysis.

H_1: There is no significant difference in the pre-test and post-test scores on cyber safety and security awareness between male and female teachers.

Table 4.1: Cyber Safety and Security Awareness (CSSA) with respect to male and female teachers

Gender		N	Mean	Std. Deviation	t	sig
PRE-TEST	**Male**	311	49.53	9.733	2.216	0.027
	Female	159	51.55	8.590		
POST-TEST	**Male**	311	55.90	10.504	2.522	0.012
	Female	159	58.34	8.664		

From Table 4.1 the data shows that in both pre-test and post-test assessment, Female participants scored significantly higher than male participants. The statistical significance is indicated by the t-tests (p-values of 0.027 for the pre-test and 0.012 for the post-test). The results imply that, on average, females performed better than males in both assessments, with a more pronounced difference observed in the post-test scores.

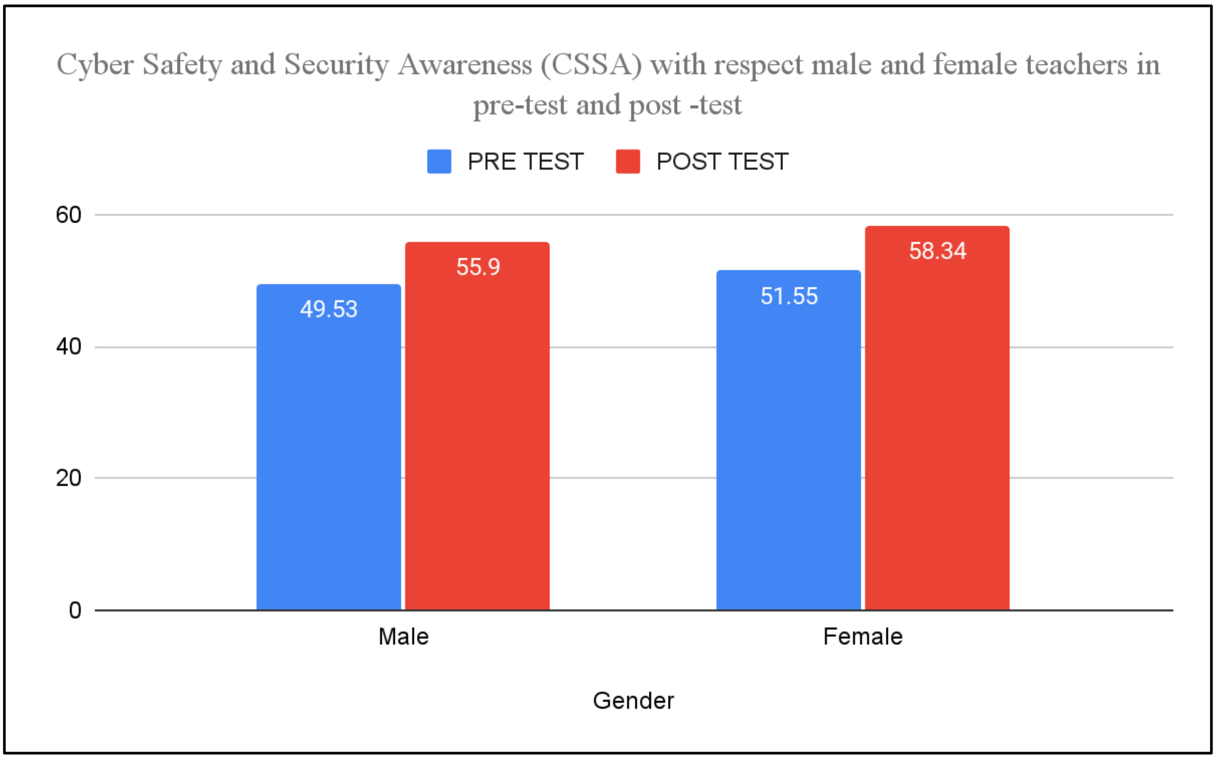


Fig 4.1 Cyber Safety and Security Awareness (CSSA) with respect to males and females in Pre-test and Post-test

H_2: There is no significant difference in the pre-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

Table 4.2: Cyber Safety and Security Awareness (CSSA) with respect to male and female teachers in the pre-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
PRE-TEST S1 TOTAL	Male	311	6.13	1.509	-2.757	0.006
	Female	159	6.53	1.479		
PRE-TEST S2 TOTAL	Male	311	8.46	1.312	-0.337	0.736
	Female	159	8.50	1.018		
PRE-TEST S3 TOTAL	Male	311	7.09	1.960	0.413	0.680
	Female	159	7.01	1.852		

PRE-TEST S4 TOTAL	Male	311	6.05	1.428	-2.094	0.037
	Female	159	6.34	1.330		
PRE-TEST S5 TOTAL	Male	311	5.52	1.812	-2.369	0.018
	Female	159	5.92	1.659		
PRE-TEST S6 TOTAL	Male	311	7.42	2.336	-1.788	0.074
	Female	159	7.81	1.972		
PRE-TEST S7 TOTAL	Male	311	4.58	1.922	-2.089	0.037
	Female	159	4.96	1.753		
PRE-TEST S8 TOTAL	Male	311	4.19	1.983	-1.417	0.157
	Female	159	4.45	1.813		
PRE-TEST	Male	311	49.53	9.733	-2.216	0.027
	Female	159	51.55	8.590		

From the above table 4.2, the overall pre-test results showed that females consistently scored higher than males. Statistically significant differences were observed in several sections: S1, S4, S5, and S7, where females had higher mean scores compared to males, with p-values below 0.05 indicating that these differences are unlikely due to chance. The overall pre-test also showed a significant difference, reinforcing the trend that females performed better than males.

H_3: There is no significant difference in the post-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

Table 4.3: Cyber Safety and Security Awareness (CSSA) with respect to male and female teachers in the post-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
POST-TEST S1 TOTAL	Male	311	6.97	1.646	-3.111	0.002
	Female	159	7.44	1.296		

POST-TEST S2 TOTAL	Male	311	8.82	1.003	-0.761	0.447
	Female	159	8.89	0.656		
POST-TEST S3 TOTAL	Male	311	7.69	1.880	-0.866	0.387
	Female	159	7.84	1.478		
POST-TEST S4 TOTAL	Male	311	6.91	1.276	-2.514	0.012
	Female	159	7.23	1.282		
POST-TEST S5 TOTAL	Male	311	6.19	1.984	-2.102	0.012
	Female	159	6.58	1.815		
POST-TEST S6 TOTAL	Male	311	8.42	1.880	-2.028	0.043
	Female	159	8.77	1.519		
POST-TEST S7 TOTAL	Male	311	5.55	2.069	-1.881	0.061
	Female	159	5.91	1.833		
POST-TEST S8 TOTAL	Male	311	5.08	2.245	-2.030	0.043
	Female	159	5.53	2.252		
POST-TEST	Male	311	55.90	10.504	-2.522	0.012
	Female	159	58.34	8.664		

From the above table 4.3, the result showed that females generally outperformed males in several sections and the overall test. Specifically, females scored significantly higher than males in the following sections: S1 (p-value = 0.002), S4 (p-value = 0.012), S5 (p-value = 0.012), S6 (p-value = 0.043), and S8 (p-value = 0.043). These p-values indicate that the differences are statistically significant and unlikely due to chance.

H_4: There is no significant difference between male and female teachers in their pre-test scores with regard to the Concept of Cyber Safety and Security information.

Table 4.4: Concept of Cyber Safety and Security Awareness with respect to male and female teachers in the pre-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which of the following is not a best practice with respect to cyber safety and security?	Male	311	0.71	0.454	-0.431	0.667
	Female	159	0.73	0.446		

Ayesha received a message that her school account was compromised and thus needed to be protected. She was asked to click on the link provided and fill in her login credentials on the web page to ensure security. The message also had a phone number that she could call to verify the message. What should Ayesha do?	Male	311	0.50	0.501	-0.871	0.384
	Female	159	0.54	0.500		
Which of the following is an important element of the educational ecosystem that can also be a reason for making other elements vulnerable and at risk?	Male	311	0.26	0.438	-0.885	0.377
	Female	159	0.30	0.458		
Anuj is a bright student in your class, his parents approached you and shared that Anuj stayed up late at night due to his habit of checking his social media accounts. They also shared that when they express their concern; he loses his temper and becomes violent. What action would you suggest to be taken by parents?	Male	311	0.51	0.501	-0.478	0.633
	Female	159	0.53	0.500		
You came across a call that asks you to scan a QR code to claim cashback of ₹2000/- on your recent purchase through your credit card. Which of the following statements is valid and thus ensures safety with respect to the situation above?	Male	311	0.73	0.446	1.352	0.177
	Female	159	0.67	0.473		
Which of the following activities is essential to ensure that the users of the system maintain confidentiality?	Male	311	0.13	0.339	-2.305	0.022
	Female	159	0.21	0.411		
Which of the following activities is part of maintaining integrity?	Male	311	0.27	0.445	-0.440	0.660
	Female	159	0.29	0.455		

Which of the following ensures maintaining the availability of resources?	Male	311	0.39	0.488	-1.398	0.163
	Female	159	0.45	0.499		
Which of the following is a negative impact of the virtual world?	Male	311	0.53	0.500	-1.973	0.049
	Female	159	0.62	0.486		
What does the CIA triad stand for?	Male	311	0.56	0.497	-1.114	0.266
	Female	159	0.62	0.488		
PRE-TEST S1 TOTAL	Male	311	4.58	1.922	-2.089	0.037
	Female	159	4.96	1.753		

From Table 4.4, the results showed that females generally had a better understanding of cyber safety and security compared to males. For example, females were more aware of the negative impacts of the virtual world and the importance of maintaining confidentiality. They also performed better in identifying unsafe actions, like phishing scams. Overall, females showed a clearer understanding of cybersecurity topics.

H_5: There is no significant difference between male and female teachers in their pre-test scores with regard to the Device Safety and Security domain.

Table 4.5: Device Safety and Security domain with respect to male and female teachers in the pre-test scores

Gender		**N**	**Mean**	**Std.Deviation**	**t**	**sig**
Why do we need to keep our devices safe and secure?	Male	311	0.95	0.215	-1.201	0.230
	Female	159	0.97	0.157		
What's a good way to make sure our device is safe?	Male	311	0.92	0.267	0.861	0.390
	Female	159	0.90	0.302		
Why should we update our device software?	Male	311	0.99	0.098	-0.374	0.708
	Female	159	0.99	0.079		
How can we stay safe on public Wi-Fi?	Male	311	0.21	0.407	2.776	0.006
	Female	159	0.11	0.310		
What does antivirus software do on a device?	Male	311	0.93	0.262	0.300	0.764
	Female	159	0.92	0.275		

What's a good way to stop others from getting into our devices?	Male	311	0.85	0.356	-0.843	0.400
	Female	159	0.88	0.325		
Why is it important to be careful with USB drives?	Male	311	0.87	0.335	0.849	0.396
	Female	159	0.84	0.365		
Why should we be careful downloading apps from other places?	Male	311	0.94	0.234	-0.937	0.349
	Female	159	0.96	0.191		
How can we keep our devices safe from getting broken?	Male	311	0.85	0.359	-2.789	0.005
	Female	159	0.94	0.244		
Why is it important to have different passwords for our accounts?	Male	311	0.95	0.221	-2.083	0.038
	Female	159	0.99	0.112		
PRE-TEST S2 TOTAL	Male	311	8.46	1.312	-0.337	0.736
	Female	159	8.50	1.018		

From Table 4.5, the result showed that females scored significantly higher than males on questions about keeping devices safe from damage and using different passwords for accounts. For example, females had a higher score on how to protect devices from getting broken, with a t-value of -2.789 and a p-value of 0.005, and also on the importance of having different passwords, with a t-value of -2.083 and a p-value of 0.038. On other questions about device safety, like keeping devices secure and ensuring their safety, there were no significant differences between males and females. Overall, females showed a better understanding of some key areas of device safety.

H_6: There is no significant difference between male and female teachers in their pre-test scores with regard to Browser, Email Security and Digital Financial Security domains.

Table 4.6: Browser, Email Security and Digital Financial Security domain with respect to male and female teachers in the pre-test scores

Gender		N	Mean	Std. Deviation	t	sig
What does HTTPS stand for in a web browser URL?	Male	311	0.84	0.365	1.514	0.131
	Female	159	0.79	0.411		
Which of the following is a common tactic used in phishing emails?	Male	311	0.24	0.430	-0.171	0.864
	Female	159	0.25	0.435		
Which feature in a browser helps prevent tracking of online activity?	Male	311	0.66	0.474	-0.920	0.358
	Female	159	0.70	0.458		
What is the primary purpose of end-to-end encryption in emails?	Male	311	0.89	0.317	-1.974	0.049
	Female	159	0.94	0.232		
Which action is unsafe when using an ATM (Automated Teller Machine)?	Male	311	0.71	0.456	0.628	0.530
	Female	159	0.68	0.468		
What is the potential risk of downloading browser extensions/add-ons from unverified sources?	Male	311	0.83	0.379	-0.275	0.783
	Female	159	0.84	0.371		
What is the most secure way to handle suspicious emails with attachments from unknown senders?	Male	311	0.66	0.476	-0.232	0.817
	Female	159	0.67	0.473		
What is the purpose of a CVV (Card Verification Value) number on a credit/debit card?	Male	311	0.82	0.388	2.643	0.008
	Female	159	0.71	0.455		
Which action helps in preventing unauthorized access to saved passwords in a browser?	Male	311	0.65	0.478	0.037	0.971
	Female	159	0.65	0.479		
Which of the following is an example of a common email attachment that might pose a security risk?	Male	311	0.80	0.403	0.285	0.776
	Female	159	0.79	0.411		

PRE-TEST S3 TOTAL	Male	311	7.09	1.960	0.413	0.680
	Female	159	7.01	1.852		

From Table 4.6, the result showed that Females had a significantly better understanding of the primary purpose of end-to-end encryption in emails (Mean = 0.94) compared to males (Mean = 0.89), with a t-value of -1.974 and a p-value of 0.049. Conversely, males showed a better grasp of the purpose of the CVV number on credit/debit cards (Mean = 0.82) compared to females (Mean = 0.71), with a t-value of 2.643 and a p-value of 0.008. For other topics, such as the meaning of HTTPS, tactics used in phishing emails, and features to prevent tracking, and handling suspicious emails, there were no significant differences between males and females, as indicated by p-values ranging from 0.131 to 0.971. Overall, the results reveal that while there are specific areas where one gender has a better understanding than the other, many aspects of internet security knowledge are similar across genders.

H_7: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social Media and Safety domain.

Table 4.7: Social Media and Safety domain with respect to male and female teachers in the pre-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which social media platform allows you to create a profile showcasing your professional experience, skills, and education?	Male	311	0.54	0.499	-1.183	0.237
	Female	159	0.60	0.492		
Which of the following is a disadvantage of social networking?	Male	311	0.91	0.291	-0.185	0.854
	Female	159	0.91	0.284		
What is social media addiction characterized by?	Male	311	0.74	0.438	-0.431	0.667
	Female	159	0.76	0.428		
What does sexting on social media refer to?	Male	311	0.70	0.459	-0.646	0.519
	Female	159	0.73	0.446		
What is catfishing in the context of social media fraud?	Male	311	0.86	0.342	0.650	0.516
	Female	159	0.84	0.365		
Why are clickbait scams considered harmful?	Male	311	0.79	0.410	-3.039	0.003
	Female	159	0.90	0.302		
What is a common tactic used in clickbait scams?	Male	311	0.74	0.440	-1.421	0.156
	Female	159	0.80	0.402		
Why are phishing scams dangerous?	Male	311	0.79	0.410	-0.761	0.447
	Female	159	0.82	0.387		

What is a good rule to follow when posting on social media?	Male	311	0.83	0.377	-2.027	0.043
	Female	159	0.90	0.302		
Which social media platform has a `Privacy checkup` feature?	Male	311	0.52	0.500	-0.602	0.547
	Female	159	0.55	0.499		
PRE-TEST S4 TOTAL	Male	311	7.42	2.336	-1.788	0.074
	Female	159	7.81	1.972		

From Table 4.7, the analysis of social media knowledge results showed that females generally had a better understanding of certain topics compared to males. For example, females were more aware of why clickbait scams are harmful (Mean = 0.90 vs. Mean = 0.79) and had a better understanding of good practices for posting on social media (Mean = 0.90 vs. Mean = 0.83). They also showed slightly better knowledge of social media addiction and sexting, though these differences were not as significant. Overall, females had a clearer grasp of some social media-related issues, while knowledge levels were similar in other areas.

H_8: There is no significant difference between male and female teachers in their pre-test scores with regard to the Cyber Scams and Frauds domain.

Table 4.8: Cyber Scams and Frauds domain. with respect to male and female teachers in the pre-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which of the following is an example of a Social Engineering attack? "	Male	311	0.43	0.496	-2.857	0.004
	Female	159	0.57	0.496		
Which social engineering attack relies on establishing a sense of urgency or fear to manipulate victims? "	Male	311	0.27	0.445	1.639	0.102
	Female	159	0.20	0.402		
What security measures can help prevent a successful phishing attack? "	Male	311	0.39	0.489	-0.346	0.730
	Female	159	0.41	0.493		
Which of the following is a characteristic of a spear phishing attack? "	Male	311	0.30	0.457	-1.654	0.099
	Female	159	0.37	0.485		
What is the primary goal of a phishing attack? "	Male	311	0.76	0.430	-0.894	0.372
	Female	159	0.79	0.407		

Which type of social engineering attack targets high-level executives or individuals with access to valuable information? "	Male	311	0.54	0.499	-1.511	0.131
	Female	159	0.62	0.488		
What does Multi-Factor Authentication (MFA) add to the security of sensitive systems or data? "	Male	311	0.41	0.492	-0.076	0.939
	Female	159	0.41	0.493		
Which of the following is NOT a common goal of social engineering attacks? "	Male	311	0.43	0.496	1.846	0.066
	Female	159	0.35	0.477		
Which social engineering technique involves manipulating an individual's greed or desire for personal gain? "	Male	311	0.27	0.445	-0.866	0.387
	Female	159	0.31	0.463		
Key Logger is a ________________ "	Male	311	0.39	0.488	-0.874	0.382
	Female	159	0.43	0.496		
PRE-TEST S5 TOTAL	Male	311	4.19	1.983	-1.417	0.157
	Female	159	4.45	1.813		

From Table 4.8 the t-test results indicated that females have a significantly better understanding of social engineering attack examples compared to males (t = -2.857, p = 0.004). However, there are no significant differences between genders in areas such as identifying urgency-based attacks, phishing prevention, spear phishing characteristics, and the purpose of phishing attacks. Both genders have similar knowledge about Multi-Factor Authentication and other security aspects, with a near-significant difference in recognizing social engineering goals. Overall, females score higher in identifying social engineering attack types, but other aspects show no significant gender differences.

H_9: There is no significant difference between male and female teachers in their pre-test scores with regard to the physical and psychological domains.

Table 4.9: physical and psychological domain with respect to male and female teachers in the pre-test scores

Gender		N	Mean	Std. Deviation	t	sig
What are the different ways in which users' psychological health is affected by their use of digital tools?	Male	311	0.82	0.388	-0.191	0.849
	Female	159	0.82	0.382		
What is behavioural addiction?	Male	311	0.89	0.313	-1.399	0.162
	Female	159	0.93	0.255		
Which of the following is NOT a healthy digital behaviour?	Male	311	0.89	0.308	-1.538	0.125
	Female	159	0.94	0.244		
What is cyberbullying?	Male	311	0.37	0.484	0.643	0.520
	Female	159	0.34	0.475		
What is cyberstalking?	Male	311	0.74	0.440	-4.114	0.000
	Female	159	0.90	0.302		
What is a common method to take sexual advantage of an immature person?	Male	311	0.41	0.493	-0.464	0.643
	Female	159	0.43	0.497		
Students stay online and miss proper sleep. What bodily functions are affected by lack of proper sleep?	Male	311	0.02	0.138	1.100	0.272
	Female	159	0.01	0.079		
How can a teacher educate students about responsible digital behaviour?	Male	311	0.68	0.467	-2.847	0.005
	Female	159	0.81	0.397		
Which of the following promotes proper internet use?	Male	311	0.52	0.500	-0.281	0.779
	Female	159	0.53	0.500		
What is digital detox?	Male	311	0.79	0.410	-0.925	0.355
	Female	159	0.82	0.382		
PRE-TEST S6 TOTAL	Male	311	6.13	1.509	-2.757	0.006
	Female	159	6.53	1.479		

From Table 4.9, the result showed that females generally scored higher than males on certain questions related to digital behavior and safety. For instance, females had significantly higher scores on the question about "cyberstalking" with a t-value of -4.114 and a p-value of 0.000, indicating a strong and significant difference. Similarly, females scored better on "how to educate students about responsible digital behavior," with a t-value of -2.847 and a p-value of 0.005, showing a notable difference.

In contrast, there were no significant differences between males and females in their responses to questions like "the impact of digital tools on psychological health" and "cyberbullying," where the p-values were 0.849 and 0.520, respectively. This suggests that both genders had similar levels of understanding in these areas.

H$_{10}$: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

Table 4.10: Social And Ethical Aspects of Cyber Security domain with respect male and female teachers in the pre-test scores

Gender		N	Mean	Std. Deviation	t	sig
To establish a good relationship with employees, customers, clients, and the general public there has to be an element of ……. in the relationship.	Male	311	0.34	0.476	-3.101	0.002
	Female	159	0.49	0.501		
Ethics is about I. Doing good for the society II. Being good III. Using tech all the time IV. Staying away from devices	Male	311	0.74	0.438	-1.822	0.069
	Female	159	0.82	0.387		
Which of the following is unethical?	Male	311	0.83	0.377	-1.079	0.281
	Female	159	0.87	0.340		
Your student has used his cousin's phone to make blank calls to another friend. What are your feelings on learning this?	Male	311	0.81	0.390	-1.860	0.064
	Female	159	0.88	0.325		
What do you call a set of suggested online behaviours that allows digital users to safely	Male	311	0.10	0.300	-0.032	0.974

enjoy surfing without causing harm to themselves and others?	Female	159	0.10	0.302		
What do you call the use of proprietary software for which the user has not paid any money?	Male	311	0.53	0.500	0.691	0.490
	Female	159	0.50	0.502		
Find the best word among the below options to describe the situation- When you copy from external sources without giving proper credit	Male	311	0.44	0.497	-2.328	0.020
	Female	159	0.55	0.499		
Two students get into a quarrel and are brought to the Head Teacher’s room. While disciplining them, the Head Teacher can also use the opportunity to teach ethics by stating	Male	311	0.71	0.453	-2.466	0.014
	Female	159	0.82	0.387		
Doxxy is an unethical behaviour. It means	Male	311	0.27	0.443	1.880	0.061
	Female	159	0.19	0.392		
Your uncle sent you a home remedy for curing diabetes. It is supposed to do wonders and reduce sugar levels. What will you do?	Male	311	0.74	0.441	0.590	0.556
	Female	159	0.71	0.455		
PRE-TEST S7 TOTAL	Male	311	5.52	1.812	-2.369	0.018
	Female	159	5.92	1.659		

From Table 4.10, the result showed that females generally showed a better understanding of ethics compared to males. For example, females scored higher on questions about maintaining good relationships (Mean = 0.49 vs. Mean = 0.34) and recognizing unethical behavior (Mean = 0.87 vs. Mean = 0.83). They were also better at understanding concepts like plagiarism and teaching ethics to students. However, there were no significant differences between males and females in areas like handling unsolicited advice or understanding proprietary software. Overall, females had a clearer grasp of ethical issues.

H11: There is no significant difference between male and female teachers in their pre-test scores with regard to the Legal Frameworks for the Cybersecurity domain.

Table 4.11: Legal Frameworks for the Cybersecurity domain with respect male and female teachers in the pre-test scores

Gender		N	Mean	Std. Deviation	t	sig
Cybercrime is __________ subject.	Male	311	0.07	0.251	1.017	0.310
	Female	159	0.04	0.206		
Cyberstalking can happen with	Male	311	0.95	0.215	0.669	0.504
	Female	159	0.94	0.244		
We can report cybercrime at	Male	311	0.77	0.420	1.882	0.060
	Female	159	0.69	0.463		
What is a personal data breach?	Male	311	0.46	0.499	0.014	0.989
	Female	159	0.46	0.500		
Which of the following is true	Male	311	0.46	0.499	-2.384	0.018
	Female	159	0.57	0.496		
Which of the following APPs is banned in India	Male	311	0.90	0.304	-0.965	0.335
	Female	159	0.92	0.265		
Cyberbullying can happen to	Male	311	0.91	0.287	-1.800	0.073
	Female	159	0.96	0.206		
Online Cyberbullying should be prevented by	Male	311	0.84	0.371	-2.680	0.008
	Female	159	0.92	0.265		
Generally, the target of online grooming is	Male	311	0.25	0.434	-2.869	0.004
	Female	159	0.38	0.486		
DPDP Act does not apply to	Male	311	0.45	0.499	0.011	0.991
	Female	159	0.45	0.499		
PRE-TEST S8 TOTAL	Male	311	6.05	1.428	-2.094	0.037
	Female	159	6.34	1.330		

From the above table 4.11, the analysis showed the cybercrime and safety knowledge, females generally had a better understanding of topics such as the truth about certain statements, preventing online cyberbullying, and the general target of online grooming. For instance, females scored higher on knowing how to prevent online cyberbullying (Mean = 0.92) compared to males (Mean = 0.84) and were more aware of the target of online grooming (Mean = 0.38 vs. Mean = 0.25). However, there were no significant differences between males and females in understanding how to report cybercrime or the applicability of the DPDP Act. Overall, females showed better knowledge in specific areas of cyber safety.

H_{12}: There is no significant difference between male and female teachers in their post-test scores with regard to the Concept of Cyber Safety and Security information.

Table 4.12: **Concept of Cyber Safety and Security information with respect to male and female teachers in the post-test scores**

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which of the following is not a best practice with respect to cyber safety and security?	Male	311	0.83	0.379	-1.914	0.056
	Female	159	0.89	0.310		
Ayesha received a message that her school account was compromised and thus needed to be protected. She was asked to click on the link provided and fill in her login credentials on the web page to ensure security. The message also had a phone number that she could call to verify the message. What should Ayesha do?	Male	311	0.59	0.493	-1.650	0.100
	Female	159	0.67	0.473		
Which of the following is an important element of the educational ecosystem that can also be a reason for making other elements vulnerable and at risk?	Male	311	0.40	0.490	-3.086	0.002
	Female	159	0.55	0.499		
Anuj is a bright student in your class, his parents approached you and shared that Anuj stayed up late at night due to his habit of checking his social media accounts. They also shared that when they express their concern; he loses his temper and becomes violent. What	Male	311	0.61	0.489	-1.933	0.054
	Female	159	0.70	0.461		

action would you suggest to be taken by parents?						
You came across a call that asks you to scan a QR code to claim cashback of ₹2000/- on your recent purchase through your credit card. Which of the following statements is valid and thus ensures safety with respect to the situation above?	Male	311	0.78	0.412	1.033	0.054
	Female	159	0.74	0.439		
Which of the following activities is essential to ensure that the users of the system maintain confidentiality?	Male	311	0.21	0.405	-1.130	0.259
	Female	159	0.25	0.435		
Which of the following activities is part of maintaining integrity?	Male	311	0.29	0.454	-0.281	0.779
	Female	159	0.30	0.461		
Which of the following ensures maintaining the availability of resources?	Male	311	0.40	0.490	0.713	0.476
	Female	159	0.36	0.483		
Which of the following is a negative impact of the virtual world?	Male	311	0.65	0.479	1.301	0.194
	Female	159	0.58	0.494		
What does the CIA triad stand for?	Male	311	0.80	0.400	-1.634	0.103
	Female	159	0.86	0.346		
POST-TEST S1 TOTAL	Male	311	5.55	2.069	-1.881	0.061
	Female	159	5.91	1.833		

From Table 4.12, the t-test results indicate that females scored significantly higher than males on questions about identifying important elements of the educational ecosystem that can create vulnerabilities (t = -3.086, p = 0.002) and on understanding suggested actions for parents dealing with students' social media use (t = -1.933, p = 0.054), which is marginally significant. Other comparisons did not show significant differences.

H_{13}: There is no significant difference between male and female teachers in their post-test scores with regard to the Device Safety and Security domain.

Table 4.13: **Device Safety and Security domain with respect to male and female teachers in the post-test scores**

Gender		N	Mean	Std. Deviation	t	sig
Why do we need to keep our devices safe and secure?	Male	311	0.98	0.138	-1.765	0.078
	Female	159	1.00	0.000		
What's a good way to make sure our device is safe?	Male	311	0.95	0.208	0.550	0.583
	Female	159	0.94	0.232		
Why should we update our device software?	Male	311	0.98	0.149	-1.286	0.199
	Female	159	0.99	0.079		
How can we stay safe on public Wi-Fi?	Male	311	0.20	0.403	1.537	0.125
	Female	159	0.14	0.353		
What does antivirus software do on a device?	Male	311	0.97	0.177	-0.830	0.407
	Female	159	0.98	0.136		
What's a good way to stop others from getting into our devices?	Male	311	0.94	0.240	-0.765	0.445
	Female	159	0.96	0.206		
Why is it important to be careful with USB drives?	Male	311	0.96	0.200	0.718	0.473
	Female	159	0.94	0.232		
Why should we be careful downloading apps from other places?	Male	311	0.97	0.168	-1.611	0.108
	Female	159	0.99	0.079		
How can we keep our devices safe from getting broken?	Male	311	0.89	0.317	-1.974	0.049
	Female	159	0.94	0.232		
Why is it important to have different passwords for our accounts?	Male	311	0.98	0.138	-0.531	0.595
	Female	159	0.99	0.112		
POST-TEST S2 TOTAL	Male	311	8.82	1.003	-0.761	0.447
	Female	159	8.89	0.656		

From Table 4.13, the t-test results showed minimal differences between males and females regarding device security knowledge. Both genders have a similar understanding of most topics, such as keeping devices safe, updating software, and using antivirus programs. However, females scored higher in their awareness of why it's important to keep devices safe from physical damage (t = -1.974, p = 0.049). The overall scores on the post-test are very close, with females slightly outperforming males in device security knowledge, though the difference is not statistically significant (t = -0.761, p = 0.447).

H_{14}: There is no significant difference between male and female teachers in their post-test scores with regard to the Browser, Email Security and Digital Financial Security domain.

Table 4.14: **Browser, Email Security and Digital Financial Securitydomain with respect to male and female teachers in the post-test scores**

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
What does HTTPS stand for in a web browser URL?	Male	311	0.91	0.291	-0.883	0.377
	Female	159	0.93	0.255		
Which of the following is a common tactic used in phishing emails?	Male	311	0.41	0.493	0.715	0.475
	Female	159	0.38	0.486		
Which feature in a browser helps prevent tracking of online activity?	Male	311	0.77	0.425	0.553	0.581
	Female	159	0.74	0.439		
What is the primary purpose of end-to-end encryption in emails?	Male	311	0.94	0.240	-0.474	0.636
	Female	159	0.95	0.219		
Which action is unsafe when using an ATM (Automated Teller Machine)?	Male	311	0.77	0.422	-1.226	0.221
	Female	159	0.82	0.387		
What is the potential risk of downloading browser extensions/add-ons from unverified sources?	Male	311	0.91	0.287	-1.020	0.308
	Female	159	0.94	0.244		
What is the most secure way to handle suspicious emails with attachments from unknown senders?	Male	311	0.68	0.467	-0.784	0.433
	Female	159	0.72	0.452		

What is the purpose of a CVV (Card Verification Value) number on a credit/debit card?	Male	311	0.86	0.352	0.181	0.857
	Female	159	0.85	0.359		
Which action helps in preventing unauthorized access to saved passwords in a browser?	Male	311	0.75	0.432	-0.660	0.510
	Female	159	0.78	0.416		
Which of the following is an example of a common email attachment that might pose a security risk?	Male	311	0.70	0.457	-0.863	0.388
	Female	159	0.74	0.439		
POST-TEST S3 TOTAL	Male	311	7.69	1.880	-0.866	0.387
	Female	159	7.84	1.478		

From Table 4.14 the t-test results showed that males and females have similar knowledge about various online security topics. For most questions, such as the meaning of HTTPS, phishing tactics, and the purpose of end-to-end encryption, the differences in responses between genders are not statistically significant. However, females tend to have slightly higher scores on questions about ATM safety, browser extensions, and handling suspicious emails. Overall, the total post-test scores are close, with females scoring slightly higher than males, though this difference is not statistically significant.

H_{15}: There is no significant difference between male and female teachers in their post-test scores with regard to the social media and safety domain.

Table 4.15: **social media and safety domain with respect to male and female teachers in the post-test scores**

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which social media platform allows you to create a profile showcasing your professional experience, skills, and education?	Male	311	0.60	0.490	-0.780	0.436
	Female	159	0.64	0.481		
Which of the following is a disadvantage of social networking?	Male	311	0.95	0.221	-0.053	0.958
	Female	159	0.95	0.219		
What is social media addiction characterized by?	Male	311	0.83	0.379	-1.163	0.245
	Female	159	0.87	0.340		

What does sexting on social media refer to?	Male	311	0.85	0.356	0.444	0.657
	Female	159	0.84	0.371		
What is catfishing in the context of social media fraud?	Male	311	0.92	0.277	-2.161	0.031
	Female	159	0.97	0.175		
Why are clickbait scams considered harmful?	Male	311	0.90	0.296	-2.273	0.024
	Female	159	0.96	0.191		
What is a common tactic used in clickbait scams?	Male	311	0.83	0.377	-0.897	0.370
	Female	159	0.86	0.346		
Why are phishing scams dangerous?	Male	311	0.85	0.356	-2.267	0.024
	Female	159	0.92	0.265		
What is a good rule to follow when posting on social media?	Male	311	0.93	0.262	-1.545	0.123
	Female	159	0.96	0.191		
Which social media platform has a `Privacy checkup` feature?	Male	311	0.76	0.428	-0.818	0.414
	Female	159	0.79	0.407		
POST-TEST S4 TOTAL	Male	311	8.42	1.880	-2.028	0.043
	Female	159	8.77	1.519		

From Table 4.15 the t-test results showed that females generally have a better understanding of social media safety and fraud compared to males. For example, females scored higher on knowledge about catfishing, clickbait scams, and phishing. Overall, females had higher post-test scores (mean = 8.77) than males (mean = 8.42), with statistically significant differences in some areas.

H_{16}: There is no significant difference between male and female teachers in their post-test scores with regard to the cyber scams and frauds domain.

Table 4.16: **cyber scams and frauds domain with respect to male and female teachers in the post-test scores**

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Which of the following is an example of a Social Engineering attack? "	Male	311	0.65	0.478	-2.477	0.014
	Female	159	0.76	0.428		

Which social engineering attack relies on establishing a sense of urgency or fear to manipulate victims? "	Male	311	0.22	0.416	-1.169	0.243
	Female	159	0.27	0.446		
What security measures can help prevent a successful phishing attack? "	Male	311	0.48	0.500	0.732	0.465
	Female	159	0.44	0.498		
Which of the following is a characteristic of a spear phishing attack? "	Male	311	0.43	0.496	-1.292	0.197
	Female	159	0.50	0.502		
What is the primary goal of a phishing attack? "	Male	311	0.76	0.427	1.062	0.289
	Female	159	0.72	0.452		
Which type of social engineering attack targets high-level executives or individuals with access to valuable information? "	Male	311	0.62	0.486	-1.253	0.211
	Female	159	0.68	0.468		
What does Multi-Factor Authentication (MFA) add to the security of sensitive systems or data? "	Male	311	0.39	0.489	-1.391	0.165
	Female	159	0.46	0.500		
Which of the following is NOT a common goal of social engineering attacks? "	Male	311	0.52	0.500	-2.039	0.042
	Female	159	0.62	0.486		
Which social engineering technique involves manipulating an individual's greed or desire for personal gain? "	Male	311	0.40	0.491	-0.536	0.592
	Female	159	0.43	0.496		
Key Logger is a ________________ "	Male	311	0.60	0.490	-1.114	0.266
	Female	159	0.65	0.477		
POST-TEST S5 TOTAL	Male	311	5.08	2.245	-2.030	0.043
	Female	159	5.53	2.252		

From Table 4.16, the t-test results indicate that females scored significantly higher than males on questions about identifying examples of social engineering attacks (t = -2.477, p = 0.014) and understanding the goals of social engineering attacks (t = -2.039, p = 0.042). Other differences were not statistically significant.

H_{17}: There is no significant difference between male and female teachers in their post-test scores with regard to the Psychological Issues in the context of Cyber Safety and Security domain.

Table 4.17: **Psychological Issues in the context of Cyber Safety and Security domain with respect to male and female teachers in the post-test scores**

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
What are the different ways in which users' psychological health is affected by their use of digital tools?	Male	311	0.88	0.328	1.236	0.217
	Female	159	0.84	0.371		
What is behavioral addiction?	Male	311	0.94	0.234	-1.940	0.053
	Female	159	0.98	0.136		
Which of the following is NOT a healthy digital behaviour?	Male	311	0.95	0.215	-1.570	0.117
	Female	159	0.98	0.136		
What is cyberbullying?	Male	311	0.27	0.443	-2.336	0.020
	Female	159	0.37	0.485		
What is cyberstalking?	Male	310	0.89	0.313	-2.392	0.017
	Female	159	0.96	0.206		
What is a common method to take sexual advantage of an immature person?	Male	311	0.82	0.385	-0.619	0.536
	Female	159	0.84	0.365		
Students stay online and miss proper sleep. What bodily functions are affected by lack of proper sleep?	Male	311	0.10	0.300	-0.245	0.807
	Female	159	0.11	0.310		
How can a teacher educate students about responsible digital behaviour?	Male	311	0.75	0.434	-3.009	0.003
	Female	159	0.87	0.340		
Which of the following promotes proper internet use?	Male	311	0.57	0.496	-0.588	0.557
	Female	159	0.60	0.492		
What is digital detox?	Male	311	0.81	0.393	-2.506	0.013
	Female	159	0.90	0.302		
POST-TEST S6 TOTAL	Male	311	6.97	1.646	-3.111	0.002
	Female	159	7.44	1.296		

From Table 4.17, the t-test results showed that there are notable differences between males and females regarding their understanding of digital health issues. Females have a significantly better understanding of how digital tools impact psychological health (t = -2.336, p = 0.020), digital detox (t = -2.506, p = 0.013), and the methods for educating students about responsible digital behavior (t = -3.009, p = 0.003). Additionally, females score higher overall on the post-test, reflecting a better grasp of various aspects related to digital behavior and health (t = -3.111, p = 0.002). However, there are no significant gender differences in understanding behavioral addiction, unhealthy digital behaviors, or the effects of sleep deprivation caused by excessive online activity.

H$_{18}$: There is no significant difference between male and female teachers in their post-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

Table 4.18: **Social And Ethical Aspects of Cyber Security domain with respect male and female teachers in the post-test scores**

Gender		N	Mean	Std. Deviation	t	sig
To establish a good relationship with employees, customers, clients, and the general public there has to be an element of ……. in the relationship.	Male	311	0.41	0.493	-1.566	0.118
	Female	159	0.49	0.501		
Ethics is about I. Doing good for the society II. Being good III. Using tech all the time IV. Staying away from devices	Male	311	0.82	0.388	-0.024	0.981
	Female	159	0.82	0.387		
Which of the following is unethical?	Male	311	0.86	0.346	-1.579	0.115
	Female	159	0.91	0.284		
Your student has used his cousin's phone to make blank calls to another friend. What are your feelings on learning this?	Male	311	0.91	0.287	-1.532	0.126
	Female	159	0.95	0.219		
What do you call a set of suggested online behaviors that allows digital users to safely enjoy surfing without causing harm to themselves and others?	Male	311	0.15	0.356	0.843	0.400
	Female	159	0.12	0.325		

What do you call the use of proprietary software for which the user has not paid any money?	Male	311	0.60	0.490	-0.052	0.959
	Female	159	0.60	0.491		
Find the best word among the below options to describe the situation- When you copy from external sources without giving proper credit	Male	311	0.57	0.496	-4.365	0.000
	Female	159	0.77	0.424		
Two students get into a quarrel and are brought to the Head Teacher's room. While disciplining them, the Head Teacher can also use the opportunity to teach ethics by stating	Male	311	0.81	0.393	-1.574	0.116
	Female	159	0.87	0.340		
Doxxy is an unethical behaviour. It means	Male	311	0.28	0.451	1.466	0.143
	Female	159	0.22	0.416		
Your uncle sent you a home remedy for curing diabetes. It is supposed to do wonders and reduce sugar levels. What will you do?	Male	311	0.78	0.416	-1.491	0.137
	Female	159	0.84	0.371		
POST-TEST S7 TOTAL	Male	311	6.19	1.984	-2.102	0.036
	Female	159	6.58	1.815		

From Table 4.18 the t-test results showed that females generally have a better understanding of digital ethics and responsible technology use compared to males. For example, females scored higher in recognizing unethical behaviors like plagiarism, with a significant difference (t = -4.365, p < 0.001). They also demonstrated a greater awareness of ethical issues and appropriate use of technology, as reflected in their overall higher post-test scores (mean = 6.58) compared to males (mean = 6.19), with a t-value of -2.102 and a p-value of 0.036. These results suggest that females have a more developed understanding of these topics.

H19: There is no significant difference between male and female teachers in their post-test scores with regard to the legal framework for the cybersecurity domain.

Table 4.19: Legal framework for the cybersecurity domain with respect to male and female teachers in the post-test scores

Gender		**N**	**Mean**	**Std. Deviation**	**t**	**sig**
Cybercrime is ___________ subject.	Male	311	0.38	0.485	2.156	0.032
	Female	159	0.28	0.449		
Cyberstalking can happen with	Male	311	0.90	0.300	0.860	0.390
	Female	159	0.87	0.333		
We can report cybercrime at	Male	311	0.98	0.149	0.179	0.858
	Female	159	0.97	0.157		
What is a personal data breach?	Male	311	0.58	0.495	-0.849	0.396
	Female	159	0.62	0.488		
Which of the following is true	Male	311	0.58	0.494	-2.744	0.006
	Female	159	0.71	0.455		
Which of the following APPs is banned in India	Male	311	0.94	0.234	-0.632	0.528
	Female	159	0.96	0.206		
Cyberbullying can happen to	Male	311	0.90	0.304	-0.736	0.462
	Female	159	0.92	0.275		
Online Cyberbullying should be prevented by	Male	311	0.92	0.272	-1.765	0.078
	Female	159	0.96	0.191		
Generally, the target of online grooming is	Male	311	0.57	0.496	-2.804	0.005
	Female	159	0.70	0.458		
DPDP Act does not apply to	Male	311	0.39	0.488	0.179	0.858
	Female	159	0.38	0.486		
POST-TEST S8 TOTAL	Male	311	6.91	1.276	-2.514	0.012
	Female	159	7.23	1.282		

From Table 4.19 the t-test results revealed some gender-based differences in understanding cyber-related topics. Females scored higher than males on several questions, including the nature of personal data breaches, the truth about certain cyber facts, and the targets of online grooming. Specifically, females were more knowledgeable about certain aspects of cyberbullying and online grooming. Males scored higher on identifying the subject of cybercrime. Overall, females scored slightly higher in the total post-test, indicating a somewhat better grasp of these cyber safety and security concepts.

4.3 Conclusion

The results and analysis of the study demonstrate that the Cyber Safety and Security Awareness Package for teachers is highly effective. Data from the online survey showed significant improvements in teachers' knowledge, confidence, and behaviors related to cyber safety and security. Post-training, teachers exhibited a substantial increase in their understanding of cyber threats and safe online practices. They reported feeling more confident in navigating the digital landscape safely and educating their students about cyber safety, which is crucial for a secure online learning environment. The training also led to positive behavioral changes, with more teachers adopting safer practices and being vigilant about potential cyber threats. Many teachers successfully integrated the knowledge from the awareness package into their teaching curriculum, enhancing student awareness and safety. Statistical analysis confirmed these findings, showing significant differences in pre- and post-training survey results, indicating the training's measurable impact. These improvements were consistent across different demographics, highlighting the package's broad applicability. The study's positive outcomes suggest that the Cyber Safety and Security Awareness Package is a valuable tool for teacher training, leading to safer online practices among both teachers and students. Educational policymakers should consider adopting such programs to enhance cyber safety in schools. Overall, the study confirms that the awareness package effectively improves teachers' cyber safety and security knowledge, confidence, and behaviors, promoting a safer digital environment in educational settings.

CHAPTER 5: SUMMARY AND CONCLUSION

5.1 Genesis of the Problem

To give teachers the tools they need to protect themselves and their students from cyber threats, the genesis of the problem in studying the effectiveness of cyber safety and security awareness packages is rooted in several key issues. The rising integration of digital technologies into education has put teachers in greater danger of data breaches, cyberattacks, and other online hazards. However, a lot of teachers lack the necessary training in cyber safety procedures, which makes them unprepared to deal with these issues. The integrity of educational operations as well as the security of sensitive student information may be jeopardized by this lack of readiness. To solve this issue, it is necessary to thoroughly assess the state of the awareness programs to make sure that teachers are adequately prepared to handle and reduce cyber threats.

5.2 Need and Significance of the Study

Digital technology now plays a crucial role in education, presenting both possibilities and difficulties. The growing threat of cyberattacks on educational institutions is one of the most urgent issues. Schools are increasingly becoming targets for cyber threats like phishing, ransomware, data breaches, and online harassment as a result of the growing use of digital technologies in the classroom. In order to safeguard themselves, their students, and the school's digital assets, teachers who are at the forefront of this digital shift - must be knowledgeable about cyber safety procedures.

Despite the crucial significance of cyber safety, a large number of teachers lack adequate training in this domain, which renders them severely lacking in their capacity to properly manage and secure digital information. This lack of readiness may leave gaps that could lead to harmful assaults on private student and school data. Teachers must be aware of these standards in order to guarantee compliance and safeguard sensitive data, as educational institutions are subject to strict privacy and data protection laws.

Yet another important factor that motivates this study's necessity is student safety. Instructors need to be prepared to teach and shield their students from cyberbullying, online harassment, and other online dangers because they are the ones who shape students' online conduct. The increasing prevalence of digital technologies in education necessitates the promotion of safe and secure technology use inside the academy.

"A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers" is significant in a number of ways. Its primary goal is to assess how well the cyber safety and security awareness package has improved teachers' knowledge of and use of cyber safety. Teachers that are more proficient in this area will be able to better manage digital settings, which will improve school security as a whole. Second, by giving educators the skills they need, the study contributes to the protection of school networks and data against cyberattacks, guaranteeing a safe learning environment.

Furthermore, policy formation is affected by the study. Researchers' findings can provide policymakers and educational authorities with information that will help them create comprehensive cyber safety regulations and teacher-specific training programmes. The larger objective of establishing a safe learning environment and encouraging confidence and trust among children, parents, and the larger school community is thereby supported by this.

Additionally, the study helps to lower the prevalence of cyberbullying and other cybercrimes by strengthening instructors' capacity to teach pupils about safe online practices, which fosters a healthy digital culture in schools. Finally, as technology develops further, instructors will be better equipped to meet new difficulties by receiving continual training and knowledge in cyber safety, which will ensure the long-term security and resilience of educational institutions.

This study concludes by addressing the urgent need for instructors to become more knowledgeable about cyber safety and security. It seeks to establish a safer, more secure learning environment for all parties concerned by assessing and enhancing the awareness package's efficacy and making sure that educators are equipped to handle the challenges of the digital era.

5.3 Statement of the Problem

The purpose of a study on the effectiveness of a cyber safety and security awareness package for teachers is to assess how well-specialized training may improve educators' understanding of and proficiency in safeguarding student information, preventing cyber threats, and maintaining a safe online learning environment. This study intends to ascertain how well the awareness package has prepared teachers in various schools in India to navigate and effectively reduce cyber dangers in educational environments.

In this context, the current research work has been undertaken and is entitled *“A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers”* has been taken up.

5.4 Operational Definitions

The terms used in this study are operationally defined as follows.

Cyber Safety and Security

According to Merriam-Webster, cyber safety is the safe practices when using the Internet to prevent personal attacks or criminal activity. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks(Kaspersky,2024). In this study, Cyber Safety and Security refer to teachers who understand how to keep themselves and their students safe online and are practising cyber safety and security. It involves educating students on how to be responsible online, accessing the internet safely, creating strong passwords, and identifying and addressing online threats including scams and cyberbullying.

Awareness

"Awareness is the quality or state of being aware: knowledge and understanding that something is happening or exists" (Merriam-Webster, 2024). In this study, an awareness for teachers is referred to as an organized educational programme designed to give instructors the knowledge, skills, and practices they need to comprehend and apply cyber safety and security measures in learning environments.

Teachers

According to Merriam-Webster, a teacher means "someone whose job is to teach in a school or college". In this study, teacher refers to an individual who is employed in an educational institution and is responsible for delivering instruction and guidance to students.

5.5 Variables of the Study

- **Independent Variable**

Variables that have undergone manipulation are considered independent variables. A variable that modifies to observe how it impacts another component is known as an independent variable. So, in this study, Gender is considered as an independent variable.

- **Dependent Variable**

A dependent variable is the measured or observed variable. This study tries to find out how the dependent variable is affected by the independent variable. In this study, the awareness of cyber safety and security is considered as the dependent variable and the study intends how the awareness varies across the selected independent variables. By observing the dependent variable, the effect of the independent variable can be measured. It was tested whether the independent variable would affect the dependent variables i.e., 'Awareness package' on Cyber Safety and Security for Teachers.

5.6 Research Question

1. What is the awareness level of teachers on cyber safety and security?
2. What are the dimensions in which teachers lack awareness of cyber safety and security?

5.7 Objectives of the Study

1. To study the awareness package of teachers on cyber safety and security.
2. To study the difference in awareness packages on cyber safety and security among teachers with respect to various subgroups.
3. To study the difference in different dimensions of cyber safety and security awareness packages among teachers with respect to various subgroups.

5.8 Hypotheses of the Study

To undertake a meaningful analysis, the following hypotheses were proposed.

H_1: There is no significant difference in the pre-test and post-test scores on cyber safety and security awareness between male and female teachers.

H_2: There is no significant difference in the pre-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_3: There is no significant difference in the post-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

H_4: There is no significant difference between male and female teachers in their pre-test scores with regard to the Concept of Cyber Safety and Security information.

H_5: There is no significant difference between male and female teachers in their pre-test scores with regard to the Device Safety and Security domain.

H_6: There is no significant difference between male and female teachers in their pre-test scores with regard to Browser, Email Security and Digital Financial Security domains.

H_7: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social Media and Safety domain.

H_8: There is no significant difference between male and female teachers in their pre-test scores with regard to the Cyber Scams and Frauds domain.

H_9: There is no significant difference between male and female teachers in their pre-test scores with regard to the physical and psychological domains.

H_{10}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{11}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Legal Frameworks for the Cybersecurity domain.

H_{12}: There is no significant difference between male and female teachers in their post-test scores with regard to the Concept of Cyber Safety and Security domain.

H_{13}: There is no significant difference between male and female teachers in their post-test scores with regard to the Device Safety and Security domain.

H_{14}: There is no significant difference between male and female teachers in their post-test scores with regard to the Browser, Email Security and Digital Financial Security domain.

H_{15}: There is no significant difference between male and female teachers in their post-test scores with regard to the social media and safety domain.

H_{16}: There is no significant difference between male and female teachers in their post-test scores with regard to the cyber scams and frauds domain.

H_{17}: There is no significant difference between male and female teachers in their post-test scores with regard to the Psychological Issues In the context of Cyber Safety and Security domain.

H_{18}: There is no significant difference between male and female teachers in their post-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

H_{19}: There is no significant difference between male and female teachers in their post-test scores with regard to the legal framework for the cybersecurity domain.

5.9 Design of the Study

The study used a survey method, a quantitative research technique that optimizes descriptive and inferential statistics, to look into teachers' awareness of cyber safety and security at the national level. This method has been selected since the intention of the study was to explore the current level of awareness of teachers about cyber safety and security. The survey research helped the researcher to get an insight into the prevailing level of teachers' awareness about cyber safety and security across the nation.

5.10 Sample

In order to conduct the research, purposive sampling was done. Twenty (20) teachers/ teacher educators were selected from each state/ UT, 100 participants representing CBSE and 5 each from other autonomous organizations. A total of 950 participants were requested to be deputed but a total of 470 individuals participated in this research study.

5.10.1 Population of the Study

The population of the present study is all the Teachers, Teacher Educators, Administrators and educational stakeholders from various States/ UTs and Autonomous Organizations like CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS. The target group also includes Teachers, Administrators and Faculty of various constituent units of NCERT like DMS, RIEs, NIE, and PSSCIVE from all 28 Indian States and 8 Union Territories. There are about 16 million teachers in the 2022-23 session (MoE, 2022) and all of them were considered as the population of the present study.

5.10.2 Sampling Technique

Sampling is the process of selecting a small group from a large population to act as that population's true representative. Sampling is the process of selecting a subset from the entire population or a predetermined sampling frame. Sampling can be used to draw conclusions about a community or to draw broad conclusions about current theories. Essentially, the selection of the sample technique determines this. Generally speaking, there are two categories of sampling techniques: Random sampling or probability and Non-random or non-probability sampling (Taherdoost, 2016).In the context of a large and geographically dispersed population, a more complex technique known as multistage sampling is employed. Multistage sampling is a complex form of cluster sampling in which the selection of samples is carried out in multiple stages (Cochran, 1977). At each stage, the population is divided into clusters or groups, and a random sample of these clusters is selected. Within each selected cluster, further sampling is done to select smaller units, and this process is repeated as necessary.

Given the vast geographical size and diversity of the population, the documented report utilized a four-phase sampling process to create the final sample for the investigation. In the first phase, the sample encompassed the entire population across all 28 states and 8 Union Territories (UTs). In the second phase, the sample included the entire population across all Autonomous organizations/ NCERT. The third phase focused on categorizing data by school type, covering CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS and DMS including their entire teacher populations. Only teachers who were using the Internet were included in the final sample for this study.

The sample was collected in two phases:

Phase 1: Selection of States and Union Territories

The first phase involved choosing every single person living in all 28 states and 8 Union Territories (UTs) in India, all 36 entities were taken. Ensuring geographic coverage and variety, this phase captured the whole range of regional variances and traits.

Table 5.1

States/UTs	Selected	Remarks
36	36	Entire Population was taken

Phase 2: Selection of School Boards/Autonomous organizations/ NCERT

In the second phase, every teacher in every state and UT across all approved school boards and Autonomous organizations/ NCERT was included in the sample. This stage was essential to creating a thorough depiction of the educational environment by incorporating the various curricula and educational systems.

Next, selecting the entire population of teachers and teacher educators from all types of schools, such as government, private, and aided which are affiliated to the state board and Central Board of Secondary Education (CBSE).

School Type	Selected	Remarks
Government & Aided Private	CBSE/KVS/NVS/ AEES / Sainik School / CISCE / EMRS /RIE/NIE/DMS/PSSCIVE	Entire Population was taken

5.10.3 Sample Size

In order to conduct the research, purposive sampling was done. Hence, all the States/UTs and autonomous organizations were requested to select and depute Teachers, Teacher Educators, Administrators and educational stakeholders. 20 participants were deputed from each state/UTs and 5 participants were deputed from each autonomous organization. The sample coverage was 470 teachers teaching in any school, whether Government, Private, or Aided school, from all 28 Indian States and 8 Union Territories.

Table 3.3 Gender-wise sample distribution

S. No.	Gender	Sample
1	Male	311
2	Female	159

5.11 Instruments Used in the Study

An awareness instrument with five aspects of cyber safety and security was developed, and validated, and reliability was achieved through pilot testing.

"It was determined to employ an online survey for data collection because of the unique nature of the study, as multiple-choice-based questions are thought to be an effective technique for gathering data in descriptive research (Lobe, Simoes, & Zaman, 2009). When collecting information from a large sample, multiple-choice-based questions are a more practical and effective method (Coolican, 2004; Quinn, 2013)."

Due to the unique nature of this research project, it was hard to find the appropriate rating scale; a multiple-choice-based scale was created in order to gather relevant information from the population.

The study used an online survey method with a quantitative design; therefore, creating a tool to collect the required data was unavoidable. The research team examined a wide range of relevant literature in order to construct the tool "A study on the effectiveness of cyber safety and security awareness package for teachers" including country reports, peer-reviewed research articles from India and abroad, cyber safety and security guidelines for teachers from various national and international agencies, policy documents from India and abroad, expert opinions, etc. Dimensions were determined and developed. The scale has four dimensions:

Physical-Psychological, Legal, Socio-ethical, and Technical. Each dimension has subgroups consisting of 10 items categorized as 4 responses.

5.11.1 Pilot Study

A feasibility study, sometimes called a pilot study, is a small-scale investigation carried out before a more extensive, full-scale investigation. It serves as a trial run to evaluate the viability, usefulness, and efficacy of the techniques and protocols intended for the primary study. A pilot study was done on a small sample of teachers. A sample of 47 teachers was chosen, and the research tool was administered to them to establish the reliability, viability, usefulness, and efficacy of the research tool.

5.11.2 Validity and Reliability

Validation of Tool: The validity and reliability of the scales employed in research are critical aspects that allow the research to provide useful results. For this reason, it is important to understand how researchers appropriately assess the scales' reliability and validity (Surucu & Maslakci, 2020). A research study may comprise only part of the methodological subspace's elements, which include scientific standards, procedures, and principles. Examples of these elements are validity systems. This subspace is utilized in substantive research to establish knowledge claims and comprises information derived from methodological research (Lund, 2022).

The literature synthesis produced themes and codes for item development in scale based on worldwide and Indian research papers, reports, and policy guidelines, as well as the identified research deficit. The expert members structured the questions and items on the background variables and dimensions of the scale using the themes and codes. The scale contains five dimensions: psychological-physical, legal, socio-ethical, and technical and the concept of cyber safety. Individual Items were developed using the dimensions. The developed questions on the background variables and items under each dimension were then examined for face validity and content validity by the national-level experts. Based on their validity examination, some items were removed, and a few were added.

- **Face Validity:** Face validity was checked by the research team members first, and then by the Program Coordinator, 80 questions and 4 dimensions were finalized.
- **Content Validity**. The rating scale was validated by 7 experts in the field. Later, the panel of experts was formed based on expertise in psychology, sociology, law, and educational technology; a minimum of five years of experience in concerned fields was required. Three professors and four assistant professors constituted the panel of experts.

The experts' suggestions regarding objectivity, and suitability of items were taken into consideration. Language difficulty was removed by replacing difficult words with easy ones. In the final rating scale out of 120 items, 80 items were selected and reframed according to the need of the study and the rest were removed. All the suggestions given by experts were incorporated into the final tool. It is only after the validation; that the tool was administered to the sample.

To determine the flaws and limitations and to achieve reliability and validity of the rating scale, pilot testing was done on a small sample of 47 teachers. It enables us to refine the instrument and make necessary improvements before the final implementation. A pilot test was conducted on 47 teachers to ensure the accuracy of items and whether it addressed research questions or not.

Reliability of Research Tool:

Reliability refers to the consistency and stability of a measurement over repeated administrations or observations. A reliability score close to 1.0 indicates a high level of consistency, meaning that the measurement is highly dependable and yields similar results under consistent conditions. The statistical analysis was conducted using version 28.0 of the Statistical Package for the Social Sciences (SPSS). Cronbach's alpha was used to determine the CSSAS quality score's internal consistency. A reliability score of 0.8 was derived from statistical analyses, indicating that the measurement instrument has demonstrated exceptional reliability in the context of the research study. In research, a reliability score of 0.8 typically indicates a very high level of reliability of the tool. It also suggests that the measurement instrument or tool used in the study demonstrates an extremely high level of consistency and stability. This high-reliability score implies that the measurement is highly trustworthy and can be relied upon to produce consistent and accurate results across multiple administrations or observations.

5.12 Limitations and Constraints

This nationwide quantitative study has its own limitations. They are limited with gender, Coverage of dimensions, Research method and coverage of languages in tools.

- **Gender:** The study is limited to examining the effectiveness of the cyber safety and security awareness package for teachers with a specific focus on gender. It explores how male and female teachers perceive and benefit from the awareness package, analyzing any differences in their responses and outcomes.
- **Dimensions of Cyber Safety and Security:** The study concentrated only on four dimensions of cyber safety and security that are pertinent to teachers including Physical-Psychological, Concepts, Legal, Socio-ethical and Technical. This boundary guarantees a targeted analysis of the most important cyber safety and security concerns that affect the intended sample.
- **Research Method:** The study adopted online surveys through Google Forms and quantitative analysis.
- **Language coverage:** The tool of the study was prepared in English and Hindi.

5.13 Major Findings of The Study

H_1: There is no significant difference in the pre-test and post-test scores on cyber safety and security awareness between male and female teachers.

The findings showed that female participants scored significantly higher than male participants in both the pre-test and post-test, with statistical significance indicated by p-values of 0.027 and 0.012, likely due to differences in their performance improvements over time.

H$_2$: There is no significant difference in the pre-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

The findings from Table 4.2 show that females scored significantly higher than males in the overall pre-test and sections S1, S4, S5, and S7, with p-values below 0.05 indicating that these differences are statistically significant.

H$_3$: There is no significant difference in the post-test scores on cyber safety and security awareness between male and female teachers with regard to all sections:

- Cyber Safety and Security - Concept, Need and Scope
- Device Safety and Security
- Browser, Email Security and Digital Financial Security
- Social Media and Safety
- Cyber Scams and Frauds
- Psychological Issues In the Context of Cyber Safety and Security
- Social And Ethical Aspects of Cyber Security
- Legal Frameworks for Cybersecurity

The findings from Table 4.3 show that females generally outperformed males in several sections and the overall test, with significant differences in sections S1, S4, S5, S6, and S8, indicated by p-values ranging from 0.002 to 0.043.

H$_4$: There is no significant difference between male and female teachers in their pre-test scores with regard to the Concept of Cyber Safety and Security information.

The findings from Table 4.4 reveal that females generally had a better understanding of cyber safety and security than males, including greater awareness of the virtual world's negative impacts, the importance of confidentiality, and better performance in identifying unsafe actions like phishing scams.

H$_5$: There is no significant difference between male and female teachers in their pre-test scores with regard to the Device Safety and Security domain.

The findings from Table 4.5 show that females scored significantly higher than males on questions about keeping devices safe and using different passwords, with significant differences indicated by p-values of 0.005 and 0.038, while no significant differences were found in other areas of device safety.

H$_6$: There is no significant difference between male and female teachers in their pre-test scores with regard to Browser, Email Security and Digital Financial Security domains.

The findings from Table 4.6 indicate that females had a significantly better understanding of end-to-end encryption in emails, while males better understood the purpose of CVV numbers on credit/debit cards, with no significant gender differences in other internet security topics.

H_7: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social Media and Safety domain.

The findings from Table 4.7 show that females generally had a better understanding of social media topics, including the harms of clickbait scams and good posting practices, while knowledge levels were similar in other areas such as social media addiction and sexting.

H_8: There is no significant difference between male and female teachers in their pre-test scores with regard to the Cyber Scams and Frauds domain.

The findings from Table 4.8 reveal that females have a significantly better understanding of social engineering attack examples compared to males, while there are no significant gender differences in areas such as urgency-based attacks, phishing prevention, and Multi-Factor Authentication.

H_9: There is no significant difference between male and female teachers in their pre-test scores with regard to the physical and psychological domains.

The findings from Table 4.9 show that females scored significantly higher than males on questions about "cyberstalking" and educating students on digital behavior, with no significant gender differences on topics like "the impact of digital tools on psychological health" and "cyberbullying."

H_{10}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

The findings from Table 4.10 indicate that females generally demonstrated a better understanding of ethics, including maintaining good relationships and recognizing unethical behavior, with no significant differences in areas like handling unsolicited advice or understanding proprietary software.

H_{11}: There is no significant difference between male and female teachers in their pre-test scores with regard to the Legal Frameworks for the Cybersecurity domain.

The findings from Table 4.11 reveal that females had a better understanding of topics such as preventing online cyberbullying and the target of online grooming, while there were no significant differences in knowledge about reporting cybercrime or the DPDP Act.

H_{12}: There is no significant difference between male and female teachers in their post-test scores with regard to the Concept of Cyber Safety and Security domain.

The findings from Table 4.12 show that females scored significantly higher than males on identifying vulnerabilities in the educational ecosystem and understanding actions for parents managing students' social media use, with the latter being marginally significant, while other comparisons showed no significant differences.

H_{13}: There is no significant difference between male and female teachers in their post-test scores with regard to the Device Safety and Security domain.

The findings from Table 4.13 indicate minimal differences between males and females in device security knowledge, with both genders having a similar understanding of most topics, though females scored slightly higher in awareness of preventing physical damage to devices, but the overall difference is not statistically significant.

H_{14}: There is no significant difference between male and female teachers in their post-test scores with regard to the Browser, Email Security and Digital Financial Security domain.

The findings from Table 4.14 show that males and females have similar knowledge about online security topics, with no statistically significant differences, although females scored slightly higher on questions about ATM safety, browser extensions, and handling suspicious emails.

H_{15}: There is no significant difference between male and female teachers in their post-test scores with regard to the social media and safety domain.

The findings from Table 4.15 indicate that females generally have a better understanding of social media safety and fraud, such as catfishing, clickbait scams, and phishing, with statistically significant differences in some areas, and overall higher post-test scores compared to males.

H_{16}: There is no significant difference between male and female teachers in their post-test scores with regard to the cyber scams and frauds domain.

The findings from Table 4.16 show that females scored significantly higher than males on identifying examples of social engineering attacks and understanding their goals, while other differences were not statistically significant.

H_{17}: There is no significant difference between male and female teachers in their post-test scores with regard to the Psychological Issues In the context of Cyber Safety and Security domain.

The findings from Table 4.17 show that females have a better understanding of digital health issues like the psychological impact of digital tools, digital detox, and teaching responsible digital behavior, with higher overall post-test scores, while there are no significant gender differences in understanding behavioral addiction, unhealthy digital behaviors, or sleep deprivation effects from too much online activity.

H_{18}: There is no significant difference between male and female teachers in their post-test scores with regard to the Social And Ethical Aspects of Cyber Security domain.

The findings from Table 4.18 show that females generally have a better understanding of digital ethics and responsible technology use, including recognizing unethical behaviors like plagiarism, with higher overall post-test scores compared to males, indicating a more developed understanding of these topics.

H_{19}: There is no significant difference between male and female teachers in their post-test scores with regard to the legal framework for the cybersecurity domain.

The findings from Table 4.19 show that females generally have a better understanding of cyber-related topics like personal data breaches, cyberbullying, and online grooming, while males scored higher on identifying cybercrime subjects, with females having slightly higher overall post-test scores.

5.14 Recommendations and Implications of The Study

- Engaging Sessions: Include interactive and practical sessions to keep teachers engaged and improve their understanding of cybersecurity.
- Encourage continuous learning by integrating cybersecurity topics into ongoing professional development.
- Provide easy-to-understand resources like brochures and videos that teachers can use to educate themselves and their students.
- Invite cybersecurity experts to conduct workshops and seminars, ensuring up-to-date and comprehensive information.
- Include digital ethics in the curriculum to help teachers guide students on responsible technology use and understanding unethical behaviors.
- Use real-life scenarios to show the impact of cybersecurity breaches and the importance of preventive measures.

Impact of Enhanced Cyber Safety Training for Teachers

- Enhancing teachers' cybersecurity knowledge will create safer schools, empower educators to model and teach cyber safety effectively, inform policy development, and ultimately prepare students to navigate the digital world responsibly.

5.15 Suggestions for Further Research

- Analyze how changes in school policies on cyber safety impact the effectiveness of teacher training programs.
- To determine which type of various training methods (like online courses versus in-person workshops) to find out which are most effective.
- Analyze how different teacher demographics (e.g., age, experience) influence the success of cyber safety training programs.
- Examine how involving parents and the community in cyber safety education helps teachers and students.

REFERENCES

Adamu Abdullahi Gabra, Maheyzah Binti Sirat, Siti Hajar, Ibrahim Bukar Dauda. (2020). Cyber Security Awareness Among University Students: A Case Study. International Journal of Advance Science and Technology https://www.researchgate.net/publication/341364046_Cyber_Security_Awareness_Among_University_Students_A_Case_Study

Ahmad, F., Khairunesa, I. S. A., Jamin, J., Rosni, N., & Thulasi Palpapanadan, S. (2020). Social media usage and awareness of cyber security issues among youths. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3090-3094. https://www.warse.org/IJATCSE/static/pdf/file/ijatcse91932020.pdf

Ahmed, O. S. (2021). Teacher's awareness to develop student cyber security: A Case Study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 5148-5156. https://turcomat.org/index.php/turkbilmat/article/view/5297

Ajankar, S. S., & Nimodiya, A. R. (2021). Cyber Security: Techniques and Perspectives on Transforming-AReviewhttps://www.researchgate.net/publication/357594453_Cyber_Security_Techniques_and_Perspectives_on_Transforming_-_A_Review

Aliyu, A., Aliyu, M., Ahmad, A., & Abdullahi, S. Investigating Cybersecurity Awareness among Tertiary Institutions Students in Nigeria https://www.academia.edu/75375925/Investigating_Cybersecurity_Awareness_among_Tertiary_Institutions_Students_in_Nigeria

Aljohani, W., & Elfadil, N. (2020). Measuring Cybersecurity Awareness of Students: A Case Study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing*, *9*(6), 141-155. https://www.researchgate.net/publication/355667870_Measuring_Cyber_Security_Awareness_of_Students_A_Case_Study_at_Fahad_Bin_Sultan_University

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233-249. https://www.scirp.org/journal/paperinformation.aspx?paperid=111804

Amir, F., Iqbal, S. M., & Yasin, M. (1999, November). Effectiveness of cyber-learning. In *FIE'99 Frontiers in Education. 29th Annual Frontiers in Education Conference. Designing the Future of Science and Engineering Education. Conference Proceedings (IEEE Cat. No. 99CH37011* (Vol. 2, pp. 13A2-7). IEEE. https://www.researchgate.net/publication/3845032_Effectiveness_of_cyber-learning

Aoyama, I., Barnard-Brak, L., & Talbert, T. L. (2011). Cyberbullying among high school students: Cluster analysis of sex and age differences and the level of parental monitoring. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, *1*(1), 25-35. https://www.researchgate.net/publication/220465648_Cyberbullying_Among_High_School_Students_Cluster_Analysis_of_Sex_and_Age_Differences_and_the_Level_of_Parental_Monitoring

Arwa A. Al Shamsi. (2020). Effectiveness of Cyber Security Awareness Program for Young Children: A Case Study in UAE. International Journal of Information Technology and Language Studies https://journals.sfu.ca/ijitls/index.php/ijitls/article/view/81

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://arxiv.org/abs/1901.02672

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education.https://ecesm.net/sites/default/files/ICERI_2014.pdf

Bebber, R. J. (2017). Cyber power and cyber effectiveness: An analytic framework. *Comparative Strategy*, *36*(5), 426-436. https://www.researchgate.net/publication/321392894_Cyber_Power_and_Cyber_Effectiveness_An_Analytic_Framework

Breda, F., Barbosa, H., & Morais, T. (2017, March). Social engineering and cyber security. In *International Technology, Education and Development Conference* (Vol. 3, No. 3, pp. 106-108). https://www.academia.edu/33830548/SOCIAL_ENGINEERING_AND_CYBER_SECURITY

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*,133-155. https://www.researchgate.net/publication/322455127_Students'_Cybersecurity_Awareness_at_a_Private_Tertiary_Educational_Institution

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-39. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

Dambrosio, R. (2021). *Student online safety and security: Middle school teacher perspectives concerning safe internet use in the classroom* (Doctoral dissertation, Ph. D. dissertation, California State University, Stanislaus).

Deepalakshmi, R. (2019). Usage of social networks sites and level of awareness in cyber security: A study of college students in Chennai city. *International Journal of Multidisciplinary Research*, *9*(2), 365-377. https://www.academia.edu/45336095/USAGE_OF_SOCIAL_NETWORKS_SITES

_AND_LEVEL_OF_AWARENESS_IN_CYBER_SECURITY_A_STUDY_OF_COLLEGE_STUDENTS_IN_CHENNAI_CITY

Eleje, L. I., Metu, I. C., Ikwelle, A. C., Mbelede, N. G., Ezeugo, N. C., Ufearo, F. N., ... & Ezenwosu, N. E. (2022). Influence of cyber-security problems in digital assessment on students' assessment outcome: lecturers' perspective. *Journal of Scientific Research & Reports*, *28*(10), 11-20. https://journaljsrr.com/index.php/JSRR/article/view/1408

Elmi, A. H. (2019). *A Survey on Cyber Security awareness among university students in Mogadishu*. Technical Report. SIMAD University. https://www.researchgate.net/publication/337758796_A_Survey_on_Cyber_Security_awareness_among_university_students_in_Mogadishu

Elradi, M. D., Abdalraheem Altigani, A., & Abaker, O. I. (2020). Cyber security awareness among students and faculty members in a Sudanese college. *Electrical Science & Engineering*, *2*(2), 24-28.

Fırat, M., & Ayran, G. (2016). Üniversite öğrencileri arasında sanal zorbalık. https://avesis.ebyu.edu.tr/yayin/aabf1cad-0227-4ca8-925f-1cb8df4955b9/universite-ogrencileri-arasinda-sanal-zorbalik

Garba, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series*, *2*(1), 82-86. https://readersinsight.net/SPS/article/view/1320

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian Journal of Teacher Education (Online)*, *33*(3), 1-16. https://files.eric.ed.gov/ https://www.researchgate.net/publication/49284978_Confronting_the_Pedagogical_Challenge_of_Cyber_Safety

Karagozlu, D. (2020). Determination of cyber security ensuring behaviours of pre-service teachers. *Kıbrıslı Eğitim Bilimleri Dergisi*, *15*(6), 1698-1706 https://www.researchgate.net/publication/348149208_Determination_of_cyber_security_ensuring_behaviours_of_pre-service_teachers

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019, June). Pedagogical aspects of cyber security exercises. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 103-108). IEEE. https://www.semanticscholar.org/paper/Pedagogical-Aspects-of-Cyber-Security-Exercises-Karjalainen-Kokkonen/4798786eeb8b20650fbfcefe76580d8b85ce3d88

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

https://www.merriam-webster.com/dictionary/cybersafety

https://www.merriam-webster.com/dictionary/awareness

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(421), 11-14.

https://www.academia.edu/37910526/An_Investigation_of_University_Students_Awareness_on_Cyber_Security

Khan, M., & Haque, S. (2017). Cyber Security and Ethics on Social Media. *Journal of Modern Developments in Applied Engineering & Technology Research*, *1*(2), 51-58.

Khurana, S. A. Review paper on cyber security. *Int. J. Eng. Res. Technol.(IJERT) ISSN*, 2278-0181. https://www.ijert.org/a-review-paper-on-cyber-security?unapproved=15885&moderation-hash=5bfa924253d23aa35e8115416bc361cf

Lester, T. M. (2018). *An Investigation on Cyber Safety Awareness Among Teachers and Parents*. Gardner-Webb University. https://www.proquest.com/openview/5e0100d2637f6b3c4e07dc149538d643/1?pq-origsite=gscholar&cbl=18750&diss=y

Ljupco Sotiroski. (2018). Cyber Security Protection And Implementing Of Legal Framework https://www.academia.edu/41982650/CYBER_SECURITY_PROTECTION_AND_IMPLEMENTING_OF_LEGAL_FRAMEWORK

M.S.Sodha, Umesh C. Vashishtha, Asheesh Srivastava. (2022). The Rationale for Cyber Safety and Security Awareness Literacy Programs for Prospective Teachers. A Quarterly Refereed Journal of Dialogues on Education. https://www.academia.edu/75208112/The_Rationale_for_Cyber_Safety_and_Security_Awareness_Literacy_Programs_for_Prospective_Teachers

Mali, P., Sodhi, J. S., Singh, T., & Bansal, S. (2018). Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study. *International Journal of Mechanical Engineering and Technology*, *9*(2), 110-124. https://www.researchgate.net/publication/323678185_Analysing_the_awareness_of_cyber_crime_and_designing_a_relevant_framework_with_respect_to_cyber_warfare_An_empirical_study

Mamata Joshi & Asmita Udpikar (2014). *A study on Cyber Crime and Security Prevention* https://docs.google.com/document/d/1b6BakJEw0J2799vFduW05RCoMgEcXJMW/edit?usp=share_link&ouid=107776409081880161751&rtpof=true&sd=true

Moallem, A. (2018, July). Cyber security awareness among college students. In *International conference on applied human factors and ergonomics* (pp. 79-87). Springer, Cham.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge. https://scholarworks.sjsu.edu/indust_syst_eng_pub/30/

Moyo, M., Sadeck, O., Tunjera, N., & Chigona, A. (2021, December). Investigating cyber security awareness among preservice teachers during the COVID-19 pandemic. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 527-550). Cham: Springer International Publishing.

Ng, A. W. Y., & Chan, A. H. S. (2009). Different Methods of Multiple-Choice Test: Implications and Design for Further Research; Castillo O, Douglas C, Feng DD, Lee JA, editors. *Hong Kong: Int Assoc Engineers-Iaeng*.

Ngeze, L. V., Khwaja, U., & Iyer, S. (2018). Cascade model of teacher professional development: Qualitative study of the desirable characteristics of secondary trainers and role of primary trainers. In *Proceeding at the 26th International Conference on Computers in Education* (pp. 755-760). https://www.researchgate.net/publication/329251705_Cascade_Model_of_Teacher_Professional_Development_-_Qualitative_Study_of_the_Desirable_Characteristics_of_Secondary_Trainers_and_the_Role_of_Primary_Trainers

Nirmala, A. P., & Sravana, N. (2018). Analysis on Challenges and Threats in Cyber Security. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *7*(4). https://www.academia.edu/42919988/ANALYSIS_ON_CHALLENGES_AND_THREATS_IN_CYBER_SECURITY

Papathanasiou, A., Papanikolaou, A., Vlachos, V., Chaikalis, K., Dimou, M., Karadimou, M., & Katsoula, V. (2013, December). Legal and social aspects of cybercrime in Greece. In *International Conference on e-Democracy* (pp. 153-164). Springer, Cham https://www.academia.edu/17298430/Legal_and_Social_Aspects_of_Cyber_Crime_in_Greece

Parmar, S. D. (2018). Cybersecurity in India: An evolving concern for national security. *The Journal of Intelligence and Cyber Security*, *1*(1). https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf

Potgieter, P. (2019, October). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. In *ICICIS* (pp. 272-280). https://easychair.org/publications/paper/wVsR

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382. https://www.researchgate.net/publication/340714158_The_Importance_of_Cybersecurity_Education_in_School

Roque Hernández, R. V., & Juárez Ibarra, C. M. (2018). Awareness and Training to Increase Cyber-Security in University Students. *PAAKAT: revista de tecnología y sociedad*, *8*(14).https://www.researchgate.net/publication/331029567_Awareness_and_Training_to_Increase_Cyber-Security_in_University_Students

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11), 125-128.

https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security.https://www.researchgate.net/publication/331029567_Awareness_and_Training_to_Increase_Cyber-Security_in_University_Students

Shelokar, Y., & Vyawhare, S. Review on Cyber Security Situational Awareness among Parents. https://www.irjet.net/archives/V6/i11/IRJET-V6I1196.pdf

Shikha Panwar & Mona Purohit. (2018). Cyber Security Awareness Challenge: In India. *International Research Journal of Engineering and Technology (IRJET)*

Shivani Ghundare, Akshada Patil, Rashmi Lad. (2020). Importance of Cyber Security. *International Journal of Engineering Research & Technology (IJERT)* https://www.ijert.org/importance-of-cyber-security

Singh, M., & Singh, A. K. Awareness and Protection Against Cyber Threats. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(6), 1531-1534.https://www.academia.edu/9202407/Awareness_and_Protection_Against_Cyber_Threats

Smith, P. K., Thompson, F., & Davidson, J. (2014). Cyber safety for adolescent girls: bullying, harassment, sexting, pornography, and solicitation. *Current opinion in obstetrics and gynecology*, *26*(5), 360-365. https://eprints.mdx.ac.uk/14022/1/Smith%20Thompson%20Davidson%202014.pdf

Sridevi, K. V. (2020). Cyber security Awareness among In-service secondary school teachers of Karnataka. *Indian Journal of Educational Technology*, *2*(2), 82.

Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. *International journal of academic research in management (IJARM)*, *5*.

Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, *25*(1), 471-486.

Tosun, N., & Akcay, H. (2022). Cyberbullying/Cyber-Victimization Status, Cyberbullying Awareness, and Combat Strategies of Administrators and Teachers of Pre-School Education Institutions. *International Journal of Technology in Education and Science*, *6*(1), 44-73.

Usman, I., & Rashid, A. M. (2014). Safety Awareness Among Pre-Service Teachers of Technical and Vocational Education in Malaysia Federal Polytechnic Bernin Kebbi, Nigeria. *Middle-East Journal of Scientific Research*, *22*(5), 655-660 https://www.scribd.com/document/517713349/5#

Vural, Y., Aydos, M., & Tekerek, M. (2016, March). Protection of National Cyber Security: Awareness & Education. In *The International Conference on Computing Technology, Information Security and Risk Management (CTISRM2016)* (p. 61). https://www.academia.edu/22790797/Protection_of_National_Cyber_Security_Awareness_and_Education

Wu, Y., Edwards, W.K., & Das, S. (2022). SoK: Social Cybersecurity. *2022 IEEE Symposium on Security and Privacy (SP),* 1863-1879.

Yusuf, S., Hassan, M. S. H., & Ibrahim, A. M. M. (2019). Cyberbullying among Malaysian children based on research evidence. In *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics* (pp. 115-137). IGI global.https://www.researchgate.net/publication/345579302_Cyberbullying_Among_Malaysian_Children_Based_on_Research_Evidence

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://www.researchgate.net/publication/339273589_Cyber_Security_Awareness_Knowledge_and_Behavior_A_Comparative_Study

ANNEXURES

Annexure I: Items of Cyber Safety and Security Awareness Tool

Questions for Teachers			
Dimensions	**Parameter**	**Sub Parameter**	**Question**
Technical	Phishing	Email	Do you respond to emails that ask for your username and password Are you aware about the phishing scam Do you click on the hyperlink asking for organization details Do you check the legitimate of the email send by your staff member Do you know Google Docs are also used for phishing
	Physical Attack	Password, Protocols	Do you leave your tablet open when unattended Do you change the password of your school system regularly? Do you log -out from your official account when not in use Do you follow the cyber protocols of your organization Do you always write down your password
	Encryption	Https, email, messaging app	Do you know the difference between http and https Do you Encrypt all email by default Do you use secure messaging app for official conversation Do you use Blockchain technique for student data management Do you use VPN for sharing confidential information
	Ransomware	Antivirus, money exchange	Do you have an antivirus software installed on your PC / Mac /Mobile Do you regularly update antivirus on your system Do you know hackers can steal information in exchange of huge

			money Are you files shared with students are password protected Do you click on the link asking for money prize as a reward
	IoT vulnerabilities	Security	Do you follow the Security measures while using the online payment Do you know use of camera or microphone are spy Do you protect your connected devices while sharing data Do you check for authentication before sending file to staff members Do you remotely turn off /on device while in use
Ethical	Confidentiality	Privacy harm	Do you ever share you bank account details with anyone Do you share otp with any unknown person if asked Do you share your personal information while filling any form Do you educated students on what information should be posted and kept private Are you aware about the drawabacks of using internet by all means
	Identity	Threat	Are you aware about the cyber crime which students are exposed to Do you share your students picture on your school website Are you aware about the identity theft when using student picture for school advertisement Do you provide awarness among students about what to be posted on social media
	Accuracy	data	Do you check before posting any information on the internet Do you know the consequences of the misinformation in cyber world Does your school share accurate information on the internet Do you review what your student

			browse on the internet Are you aware about theuse of data policy in school
	Security	data security , information sharing	Do you know where our data is and how it is protected Are our employees being appropriately trained on cybersecurity Do you know how to respond in a cyber security emergency Can you detect an attempted or successful cybersecurity incident, brute force attack, or data breach Do you documented policies match what is actually happening in practice
Legal	Crime	against people	Are you aware about the law for child ponography Do you notice what your student post on their social media platform Do you limit your student access on the internet
		against property	Are you aware about hacking of the computer server Do you follow copyright mechanism for your content Are you aware about the virus transmission on your computer Do you educate youself for cybercrime
	Cyber law	Defamation	Do you share defamation cases and protection law with the students
		Contracts	Do you read terms and conditions before registering on the website
		Copyright	Do you protect your books, blogs, music you share on the internet
		Patents	Do you educate your students about how to protect new invention (developing new software) by students
		Jurisdiction	Are you aware about the different jurisdiction to report cybercrime Do you know whom to report if you face cyber security problem in school

		Data Retention	Are you aware about handling students record online safely Do you handle the students record in password protected file
Social And Psychology	Neuroticism	guilt, anger, fear, sadness	Do you educated your students against cybercrime periodically
	Extroversion	friendly	Do you perform activities with your students for cyber-awarness
	Openness	new experiences	Do you try new methodology to create cyber awarness among students
	Agreeableness	eagerness, kind	Do you council if you encounter any student who became victim of cyber bullying As a teacher do you council the students of your class to be kind and supportive with any student who is the victim of cyber crime
	Conscientiousness	self-control	Do you track the activities of your students about what they are browsing on the internet
Summary			
Dimension	**5**		
Parameter	**16**		
Sub-parameter	**22**		
Questions	**65**		
Lekart Scale	**Agree/Disagree OR Yes/NO**		

Questions for School Administrator

Dimensions	**Parameter**	**Sub Parameter**	**Question**
Technical	Phishing	Email	Do you respond to email that ask for your username and password Are you aware about the phishing scam Do you click on the hyperlink asking for organisation details Do you check the legitimate of the email send to you Do you know Google Doc are also used for phishing

	Physical Attack	Password, Protocols,	Do you leave your tabelt open when unattended Do you change password of your system on regularly basis. Do you log -out from your official account when not in use Do you follow cyber protocols of your organization Do you always write down your password
	Encryption	Https, email, messaging app	Do you know the difference between http and https Do you Encrypt all email by default Do you use secure messaging app for official conversation Do you use Blockchain technique for student data management Do you use VPN for sharing confidential information
	Ransomware	Antivirus, money exchange	Do you have an antivirus software installed on your PC / Mac /Mobile Do you regularly update antivirus on your system Do you know hackers can steal information in exchange of huge money Are you files shared with students are password protected Do you click on the link asking for money prize as a reward
	IoT vulnerabilities	Security	Do you follow the Security measures while using the online payment Do you know use of camera or microphone are spy Do you protect your connected devices while sharing data Do you check for authentication before sending file to staff members Do you remotely turn off /on device while in use
Ethical	Confidentiality	Privacy harm	Do you ever share you bank account details with anyone Do you share otp with any unknown person if asked

			Do you share your personal information while filling any form Do you have knowledge on what information should be posted and kept private Are you aware about the drawbacks of using internet by all means
	Identity	Threat	Are you aware about the cyber crime which netizens are exposed to Do you post picture of unknown person on your official website Are you aware about the identity theft when using picture for advertisement Do you provide awarness among netizens about what to be posted on social media
	Accuracy	data	Do you check before posting any information on the internet Do you know the consequences of the misinformation in cyber world Does your school share accurate information on the internet Do you review what your student browse on the internet Are you aware about the use of data policy in school
	Security	data security, information sharing	Do you know where our data is and how it is protected Are our employees being appropriately trained on cybersecurity Do you know how to respond in a cyber security emergency Can you detect an attempted or successful cybersecurity incident, brute force attack, or data breach Do you documented policies match what is actually happening in practice
Legal	Crime	against people	Are you aware about the law for child ponography Do you notice what others post on their social media platform Do you limit your student access on the internet

		against property	Are you aware about hacking of the computer server Do you follow copyright mechanism for your content Are you aware about the virus transmission on your computer Do you educate youself for cybercrime
	Cyber law	Defamation	Do you share defamation cases and protection law with the students
		Contracts	Do you read terms and conditions before registering on the website
		Copyright	Do you protect your books, blogs, music you share on the internet
		Patents	Do you educate your students about how to protect new invention (developing new software) by students
		Jurisdiction	Are you aware about the different jurisdiction to report cybercrime Do you know whom to report if you face cyber security problem in school
Social And Psychology	Neuroticism	guilt, anger, fear, sadness	Are you aware about handling students record online safely Do you handle the students record in password protected file
	Extroversion	friendly	Do you educated yourself against cybercrime periodically
	Openness	new experiences	Do you perform activities for cyber-awarness
	Agreeableness	eagerness, kind	Do you try new methodology for cyber awarness
	Conscientiousness	self-control	Do you council if you encounter any victim of cyber bullying As a administrator do you council the staff members to be kind and supportive with any student who is the victim of cyber crime
			Do you keep track record of the activities about people are browsing on the internet

Questions for Students

Dimensions	**Parameter**	**Sub Parameter**	**Question**

Technical	Phishing	Email	Do you respond to email that ask for your username and password Do you click on the email askig for prize money Do you click on the email asking for registering free online game Do you share your pictures through email with your friends Do you respond to email asking for free gaming application
	Physical Attack	Password, Protocols	Do you leave your tabelt open when unattended Do you change password of your school system on regularly basis. Do you log -out from your computer when not in use Do you follow school rules in computer lab Do you always write down your password
	Encryption	Https, email, messaging app	Do you know the difference between http and https Do you respond to SMS asking for Wining a Prize money Do you ask your parents while doing online shoping Do you always do copy and paste assignment from internet Do you share your secret information with your friends on social media platform
	Ransomware	Antivirus, money exchange	Do you have an antivirus software installed on your PC / Mac /Mobile Do you regularly update antivirus on your system Do you know hackers can steal information in exchange of huge money Are you files shared with teachers are password protected Do you click on the link asking for money prize as a reward

	IoT vulnerabilities	Security	Do you follow the Security measures while using the online payment Do you know use of camera or microphone are spy Do you protect your connected devices while sharing data Do you help your friends with homework by sending files through email Do you remotely turn off /on device while in use
Ethical	Confidentiality	Privacy harm	Do you ever share you email password details with anyone Do you share otp with any unknown person if asked Do you share your personal information while filling any form Do you know what information should be posted and kept private Are you aware about the drawabacks of using internet by all means
	Identity	Threat	Do you know sbout cyber-crime Have you seen your picture posted on your school website Did you share your emails with your parents Do your school take permission while posting your picture on social media
	Accuracy	data	Do you check before posting any information on the internet Do you know the consequences of the misinformation in cyber world Does your school share accurate information on the internet Did your parents review what your browse on the internet Are you aware about the use of data policy in school
	Security	data security, information sharing	Do you know where our data is and how it is protected Are our employees being appropriately trained on cybersecurity Do you know how to respond in a cyber

			security emergency Can you detect an attempted or successful cybersecurity incident, brute force attack, or data breach Do you documented policies match what is actually happening in practice
Legal	Crime	against people	Are you aware about the law for child ponography Do you notice what your student post on their social media platform Do you limit your student access on the internet
		against property	Are you aware about hacking of the computer server Do you know copyimg the content from internet for your homework is also cyber -crime Are you aware about the virus transmission on your computer Do you educate youself for cybercrime
	Cyber law	Defamation	Do you share with your teacher/parents if you are bullied in school
		Contracts	Do you read terms and conditions before registering on the website
		Copyright	Do you protect your books, blogs ,music you share on the internet
		Patents	Does your school educate you about how to protect new invention (developing new software)
		Jurisdiction	Are you aware about the different jurisdiction to report cybercrime Do you know whom to report if you face cyber security problem in school
Social And Psychology	Neuroticism	guilt, anger, fear, sadness	Did you share with your teacher /parents if your classmates are stalking you Do you school motivate you in sharing cyber grooming incidents
	Extroversion	friendly	Did your friends behave good with you if you mistakenly posted something wrong on your social media
	Openness	new experiences	Did your teacher play fun- activities for cyber-awarness

	Agreeableness	eagerness, kind	Are you school mates/neighours behave kind with you if you are victim of cyber -stalking
	Conscientiousness	self-control	Did your teacher restricts you to have self control on the usage of the internet
			Did your teacher track the activities about what you are browsing on the internet