Cyber Crime Awareness from the Perspective of Educators: A Conceptual Study

Dr. Ashok Kumar,

Professor Dept. of Education,
Radha Govind University
Ramgarh, Jharkhand

KEYWORDS

Awareness, Cybercrime, Security, Initiatives and Hacking

ABSTRACT

The problem of cybercrime is really serious nowadays. India's internet user base is growing quickly, which has created exciting potential in a number of industries, including entertainment, sports, education, and commerce. But this expansion has also made the country more susceptible to cyber attacks. Financial stability and security are seriously threatened by identity fraud, privacy invasion, and other types of cybercrime. All of that data Hackers worldwide continue to attack India in spite of the Technology Act of 2000's attempts to solve these problems. Fewer people are aware of the more complex forms of cybercrime, such as phishing, ransomware, and cybers talking, even if many people are acquainted with fundamental hacking and simple cyber threats. The researchers set out to determine how well-informed educators were about cybercrime, its ramifications, and their possible contribution to its mitigation. According to a literature analysis and surveys of sixty teachers, the results show that while the majority of educators are aware of cybercrime, their comprehension differs greatly, especially with relation to particular dangers. Common problems include improper usage of public Wi-Fi, privacy issues, and a lack of understanding of rules and precautions. To bridge these gaps, the paper emphasises the need for focused awareness initiatives and legal education. The study's conclusions highlight how important it is to raise knowledge of cybercrime, especially among educators, so that both they and their students may have safer online experiences. Comprehensive cyber security training should be included into teacher preparation programs in order to close the knowledge gap, safeguard private data, and equip teachers to encourage responsible online conduct.

Introduction

Education that emphasises digital literacy is becoming more vital on a global scale in the 21st century. The number of crimes connected to social media is steadily rising. Everyone has a responsibility as a citizen to be alert to the many forms of online fraud. That is why teaching cyber resilience is a top priority. Teachers in this world must possess strong cyber intelligence. The term "cybercrime" refers to illegal activities carried out on the internet that target or use computers in some way. Since many crimes change every day, it's hard to divide

them all into specific categories. Rape, murder, and theft may not always have to be considered distinct crimes, even in the actual world. It depends on the nature of the cybercrime, but in every case the victim is either the computer or the person doing it.
Therefore, for the sake of clarity, the computer will be seen as either an object of attack or a tool. People become contributing members of society as they undergo the process of education, which entails passing on the wisdom, experience, and values held by previous generations. Things like ideas, perspectives, abilities, hobbies, and values are always evolving as a result of the ever-changing nature of life itself. Here, education is all on helping the student adapt to a world that's always changing. Both new chances for criminal activity and new forms of crime are generated by technological advancements. The widespread use of technology for both constructive and harmful purposes has been facilitated by the widespread availability of inexpensive technology brought about by modernisation. A person's identity, which seems to be a solid truth, may be compromised by cybercrime, which emphasises how important networked computers are to our daily lives. A common example is hacking, which is gaining unauthorised access to a computer system and its data and resources.

Research questions of the Study

- How essential is cyber security in classroom instruction?
- How can several organisations collaborate to enhance awareness of the need for cyber security?
- In what ways may educators mitigate the incidence of cybercrime?

Cyber Crime

The wide variety of illegal actions committed via the use of computers, networks, or other digital devices is collectively known as cyber crime. Think of cybercrime as the catch-all term for all the different kinds of wrongdoing that cybercriminals engage in. Among the numerous examples of this type of attack are hacking, phishing, malware, ransomware, and identity theft. Cybercrime has no geographical limits. The globe is home to criminals, victims, and technological infrastructure. Cybercrime has several forms and is always developing as a result of the proliferation of technological methods for penetrating individual and organizational networks. Cybercrime prevention, investigation, and prosecution are, therefore, a never-ending battle with many shifting obstacles. Following the most recent breakthroughs in the computer industry and networks, the word "cybercrime" was developed as a result of these innovations. There are a number of damaging impacts that may be caused by cybercrimes, including financial losses, breaches of sensitive data, system failures, and harm to reputation. At the same time that more and more people are becoming dependent on digital devices and networks for their day-to-day operations, the threat of cybercrime is growing.
As a consequence of this, it is more essential than ever before to take measures to safeguard oneself against the threat of cybercrime. "The illegal usage of any communication device to commit or facilitate in committing any illegal act" is one definition of cybercrime. The term "cybercrime" refers to illegal activity that takes place on the Internet and specifically targets computers or networks of computers for malicious purposes. Computers and computer networks are the tools of cybercriminals. They may be aiming their attacks at specific people, companies, or even governments. When looking into devices that might be involved in or the target of a cybercrime, investigators often employ a wide variety of techniques.

Education

The Latin roots of the English word "education" include "educare," "educere," "educo," and "Educatum." To "educare" is to "nourish" or "raise," and "educere" is to "draw out" or "manifest." Literally, "educo" means "to lead out of." An "act of teaching" is what the Latin word "educum" refers to. 'Educere' signifies to bring forth or to make visible. The basic meaning of the terms "educare" and "educere" is the maturation of a child's dormant abilities. However, these alternatives are unknown to the youngster. Only a teacher or educator can

know these things and know how to help their students develop them. The word "Siksha" originates in Sanskrit and is borrowed into Hindi. To "shash" is to govern, control, direct, command, etc. Education, in its more conventional definition, entails regulating and disciplining a person's actions. There are six sub-disciplines of the Sanskrit Sutra literature, and "Shiksha" is one of them. The others are Chhanda, Byakarana, Nirukta, Jyotisha, and Kalpa. Studying the Vedas was the original purpose of the Sutra literature. Guidelines for pronouncing words are called siksha. An additional Sanskrit word clarifies the essence of schooling. Specifically, it is "Vidya" (knowledge). The word "Bid" means knowledge, which is where the name "Vidya" comes from. Perhaps we might have a better understanding of the term's nature and significance if we cite the definitions of education offered by prominent Western and Eastern educators. All round development is education.

Concept of Cybercrime

Academics have disagreed on how to define cybercrime. The Greek word "Kybernetes" is the origin of the English word "cybernetic," which in turn comes from the term "cyber," as stated by Duah. The term was first used in 1948 by Nobert Wiener to describe a "formalization of concepts of feedback with various effects for engineering systems control, computer science, philosophy, biology as well as the organization of society" (Duah, 2013). Cybercrime differs significantly from conventional crime in concept. As a result of the proliferation of internet-connected devices, this crime has received far more media coverage than more conventional forms of criminality. Cybercrime is unique, thus it's important to study it.

1. People with specialized knowledge – Because of the technological nature of cybercrime, those who commit it are required to have an exceptional level of proficiency in the use of computers, the internet, and other technologies that are of a similar nature. Cybercriminals often possess academic degrees and a comprehensive understanding of how the internet operates, which makes it challenging for law enforcement to catch them. Cybercriminals are so tough to apprehend.
2. Geographical challenges – The boundaries of the physical world were rendered meaningless in cyberspace. When a cybercriminal is seated anywhere in the world, they have the ability to swiftly launch an attack on another specific region of the world. Take for example a hacker from India who manages to gain access to a system located in the United States.
3. Virtual World – When a cybercrime is committed, even if the person who committed it is located outside of cyberspace, the crime itself takes place within cyberspace. During the commission of such a crime, the culprit conducts all of their activities online.
4. Collection of Evidence - The gathering of evidence of cybercrime and its presentation in a court of law is very challenging due to the fact that cybercrime is inherently elusive. In the course of conducting cybercrime, the perpetrator makes reference to the jurisdiction of a number of different countries while concealing themselves in a specific area.
5. Magnitude of crime unimaginable - The potential for cybercrime to cause harm and loss of life to a level that cannot even be conceived of is unfathomable. The crimes that is committed online, such as cyber terrorism and cyber pornography, have a broad reach and have the potential to damage websites and steal data from businesses in a short amount of time.

Need of the Study

Although there is no denying that the internet has greatly benefited educational institutions, there are also disadvantages. Both instructors and students, particularly younger ones, spend a great deal of time on computers. The emergence of social media, e-commerce, and easily available financial services has made the internet a worldwide platform for people from all walks of life to interact. These services attract a significant number of people, and sometimes

this attraction intensifies to the point of addiction. A growing number of pupils from the current generation have a strong interest in and a thorough comprehension of a variety of technology modalities. Their ability to operate them and their understanding of their use are excellent. However, our teachers are often criticised for their seeming lack of acquaintance with and competence with modern technology.

Many teachers are reluctant or do not take any initiative in the field of computer and internet education. Given the critical role that computers and the internet play in our modern world, it is essential that instructors foster an interest in studying these subjects. Understanding the proper and improper uses of computers is crucial for educators, particularly when it comes to internet access. An educator has to understand the difference between good and wrong while using the internet. Teachers are more equipped to assist their peers and teach their pupils safe internet use when they have a thorough grasp of online etiquette. Cybercrimes may be committed with or without knowledge. It is essential for pre-service and in-service educators to comprehend the causes that lead to cybercrime and the strategies that may be used to mitigate it. To ensure their own safety and that of their students in the digital era, teacher candidates must familiarise themselves with the threats posed by cybercrime. Educators must be vigilant about the many types of cybercrime, many of which are difficult, if not impossible, to detect. A growing number of persons are falling prey to cyber crimes perpetrated via different internet-connected devices. Enhancing cybercrime awareness among educators will facilitate the dissemination of information to the broader public on this kind of crime.

Literature Review

- Narahari and Shah assessed the awareness of cybercrimes among 100 participants in their 2016 research. They found that individuals still need more education on cyber security and cybercrimes, despite the majority of respondents possessing a fundamental comprehension of both subjects. They proposed a conceptual framework for enhancing internet users' awareness.
- Mokha (2017) establishes a definitive correlation between the increase in internet users and the rise in cybercrimes. She discovered that although most persons are aware of viruses and hackers, they lack knowledge of more complex cyber threats like as phishing, cyber speech, cyber defamation, and identity theft. The research emphasises the need of educating individuals about various types of cybercrime and enhancing cyber security protocols. The survey also examines the levels of knowledge among internet users across different age groups and educational backgrounds.
- A research titled "Cyber Security awareness among college students in Tamil Nadu" was carried out by Kumar and Easwaramoorthy in the year 2017. The data for the research was collected via the use of an online survey. A range of security concerns, including pop-up windows, password strength, email phishing, and harmful applications, are taken into consideration in order to assess the students' overall comprehension of cyber security. The percentage of college students in Tamil Nadu who are informed about cyber security is 69.45%, with 30.85% of them being female and 38.6% being male being the gender breakdown.
- This research was conducted with the intention of determining the degree to which Taiwanese instructors are able to grasp and implement cyber security measures. As a component of the quantitative technique used in this research, a questionnaire was utilised to conduct a survey of 250 Taiwanese school teachers. The results of the survey indicated that educators lacked sufficient knowledge about the various cyber security operations. After making adjustments for factors such as age, number of years of classroom experience, and school location, the researchers who conducted

the study discovered that there were no statistically significant variations in the instructors' grasp of cyber security from one another.

- Despite being digital wizards, young students often overlook the crucial lesson of guarding their personal information while surfing the wild waves of public Wi-Fi, as pointed out by Sharma and Das (2020). Who knew the internet could be such a sneaky place? Because of this little hiccup in comprehension, they might just find themselves in a pickle with risks like cyber bullying, identity theft, and stumbling upon content that's best left in the dark corners of the internet. Teacher education programs really need to step up their game with some serious cyber crime awareness initiatives! The authors are practically waving their arms, urging educators to jump into the digital safety pool and teach kids how to swim without getting eaten by the internet sharks.
- Even though teachers are practically glued to their screens, they often find themselves in a bit of a pickle when it comes to understanding the sneaky world of cybercrime, as pointed out by Patel and Bhatt (2021). Who knew that clicking 'yes' on every pop-up could be a risky business? A recent study of Indian schools revealed that most educators surveyed were blissfully unaware of the significance of strong passwords or the lurking dangers of phishing attempts. It's like leaving the front door wide open and wondering why the cookies are missing.
- In their survey, Viraja and Purandare (2021) found six problems and four effects of cybercrimes, and they proposed ways to fix them. While cybercrimes cannot be totally eliminated, they may be lessened by simple security measures and safeguards.
- In 2022, Cremer et al. This study presents the results of a systematic review that examined databases that dealt with cyber risk and cyber security. The vast majority of the datasets were found to be used for technical elements of cyber security, including intrusion detection and machine learning. Cyber risk datasets that were made accessible lacked sufficient representation. The ever-changing nature of cyber risk, along with the dearth of relevant historical data, makes it very difficult for cyber insurance stakeholders to assess and comprehend. To overcome this obstacle, researchers and cyber insurers alike need a greater density of cyber data for use in risk management and analysis. Based on data from 'Open Science' FAIR, firms and insurers might benefit from a better knowledge of cyber events, more awareness of the risks involved, and better loss prevention measures (Jacobsen et al. 2020). Researchers have been able to delve more deeply into cyber hazards because to the proliferation of data, which has improved our understanding of these threats. Businesses might use this newfound information into their company culture to decrease cyber threats.

Cyber Ethics

The term Cyber Ethics refers to the study of problems around the use of the internet. Machine, specifically how people use them and what they do with them programmed to do, and the implications this causes on individuals and societies. Secrecy refers to the safeguarding of individualised information from being distributable without payment. Cyber ethics also involves the study of ethical, regulatory, and social concerns with cyber technology. This research investigates the impact that the technology of the internet has on the social, legal, and moral institutions that we have. The social policies and regulations that have been established as a reaction to the problems that have been brought about by the development and use of cyber technology are also investigated in this report. Hence, there is a reciprocal interaction here.

Types of Cybercrime

Computer systems, computer networks, and the Internet are all examples of cybercrime, which is committed when criminals take use of these resources. There are three major

categories that may be used to classify criminal acts: those that are aimed against persons, those that target private property, and those that target the state.

- **Crimes against Persons** - Comprise activities such as cyber stalking, the dissemination of offensive content such as child pornography, the use of technology to defame individuals through hacking, and the use of technology to threaten or harass individuals.
- **Crimes against Property** - Software piracy, cyber squatting (the act of claiming domain names that are similar to one another), cyber vandalism (the act of destroying data or disrupting network services), hacking computer systems, transmitting viruses, cyber trespassing (the act of gaining unauthorized access to computers), and internet time theft are all examples of intellectual property violations.
- **Crimes against the Government** - Among them are cyber terrorism, which is defined as the act of compromising national security via the use of the internet; cyber warfare, which refers to hacking and espionage that is driven by political agendas; the distribution of pirated software; and the possession of illegal information.

Why would hackers find India easy targets?

India is vulnerable to cybercrimes due to several factors:

1. **Rapid Digitalization:** In recent years, India has seen a dramatic digital transition, one that has resulted in an increasing number of people and enterprises depending on the Internet and digital technology. More chances for cybercriminals to exploit vulnerabilities are created as a result of growing connection and dependence on technology.
2. **Large Internet User Base:** The number of people using the internet in India is among the highest in the world. Because there is a huge population that uses the internet, there are more possible targets for hackers, which make it a profitable market for cyber attacks.
3. **Lack of Awareness:** There is a significant population in India that is not completely aware of the dangers that are linked with the use of digital gadgets and the internet. Individuals and companies are more susceptible to cyber assaults when they are not aware of the best cyber security measures and the hazards that are posed by the internet.
4. **Inadequate Cyber security Infrastructure**: The infrastructure for cyber security in India is still in the process of development. Many companies, particularly smaller firms, may not have sufficient cyber security safeguards in place, which makes them ideal targets for hackers. This is especially true for smaller enterprises.
5. **Weak Legal Framework:** In spite of the fact that India has rules and regulations in place to deal with these problems, the legal structure is always changing, and it may be difficult to enforce at times. Because of this, the effective prosecution of cybercriminals may be slowed down temporarily.
6. **Technological Advancements**: In tandem with the progression of technology comes an increase in the number of cyber dangers. Hackers are always coming up with new methods to take advantage of weaknesses in computer systems, including software, hardware, and network infrastructure.
7. **Insider Threats:** Insider threats, which occur when workers or other persons who have access to sensitive information abuse it for harmful reasons, are a serious worry in India, especially in the business sector.
8. **Payment Systems Vulnerability**: Phishing, credit card fraud, and other forms of online scams are examples of the types of financial crimes that are becoming more prevalent as a result of the proliferation of digital payment methods and online transactions.

9. **Cross-Border Challenges:** As a result of the fact that cybercriminals may operate from any location on the planet, it is very difficult to catch and punish them, particularly if they are based in nations that have inadequate cyber security restrictions.

Cyber-Smart Educator Proficiency

When it comes to education, having a strong understanding of technology is comparable to having an enthusiastic guide in a virtual theme park. They are more than ready to teach their pupils the ropes while also ensuring that their students do not get lost in the craziness that exists online. The abilities that are being provided are going to be a wonderful source of joy for all members of the community, including students, parents, and other members of the community. It is comparable to a feast of information, and everyone is welcome to partake in the feast! In order for educators to succeed in the chaotic digital age, they need to acquire a number of technical abilities, communicate like professionals, solve issues at the speed of light, and adjust as elegantly as a chameleon at a dance party. In the same way as a superhero with a cape made of empathy would, they need to have a genuine understanding of the issues and objectives of the stakeholders and be able to connect to them. They must possess this degree of expert skill in order to be considered qualified.

What is Cyber Security Awareness, and Why is it Important in Education?

Cyber security awareness refers to the degree to which people are knowledgeable and comprehend the need of safeguarding digital systems and data. Acknowledging cyber dangers, comprehending the risks involved, and implementing safe procedures are all part of it. This understanding, which is usually fostered via training and continuing education, seeks to protect both people and businesses against cyber catastrophes. School districts are a prominent target for data breaches because to the abundance of personal information they have on staff, students, and parents. Therefore, it is vital for them to be prepared. In addition to the traditional methods of instruction, assessment, and parent-teacher communication, today's educators are also becoming proficient in a wide range of digital tools. Because consumers may be ill-prepared to recognize phishing or spoofing efforts on newly-introduced platforms, this kind of scenario poses a significant threat to cyber security.

Common Cyber Incidents in the Education Sector

Most elementary and secondary schools allocate less than eight percent of their budget on cyber defense, according to a new study. Attackers targeting these schools online use phishing, website spoofing, malware, or a mix of these methods to get access to sensitive student information. Given the increasing reliance on software for school operations, ransomware has emerged as another prevalent cyber threat in the education sector. Administrators may be coerced into giving in to hackers' demands if they lock down their network, which would drag the whole institution to a crawl.

Phishing

There are several ways in which education software is meant to keep teachers informed, whether it is via the submission of work by a student or through the communication of a parent. Due to the fact that these notifications are almost always sent out by email, cybercriminals have a significant opportunity to imitate the messages that are sent out by these platforms in order to trick teachers and administrators into clicking on harmful links by mistake.

Spoofing

As a result of the fact that digital transformation is linked with the use of new and unfamiliar platforms, consumers are sometimes unable to notice the subtle indicators of spoofing. To bring a whole school network to its knees in a short amount of time, something as simple as stolen login credentials may be accomplished.

Ransomware

It is becoming more common for educational institutions to rely on software for their operations. Despite the fact that this presents a number of advantages to both students and instructors, it also makes educational institutions more appealing targets for cybercriminals, particularly in the case of ransomware attacks. As a result of the fact that ransomware attacks have been experienced by 44% of schools, Intel has determined that this form of cyber attack vector is the most prevalent in the educational sector. In the event that a data breach occurs, all of these assaults have the potential to have detrimental consequences on the efficiency with which a school teacher, as well as to inflict long-lasting implications on the privacy of students. Once educators and administrators have received the appropriate training to identify these cyber risks, it is a relief to know that all of them have immediately detectable indications. Cyber security awareness training is sometimes the only method that can be used to defend against attacks such as phishing. This training imparts the necessary information to your user base, allowing them to identify when an attack is taking place.

The Importance of Cyber Crime Awareness for Future Teachers

Cybercrime poses a significant threat to educational institutions and children, ranging from cyber bullying to extensive data breaches. Educational institutions are increasingly vulnerable to cyber threats due to their dependence on digital technology for communication, administration, and educational purposes. In the event of a data breach, there is a risk that records of students, financial information, and the names and contact details of faculty and staff members could be compromised. Such breaches can lead to significant disruptions in school operations, financial losses, and jeopardise the safety of both personnel and students. Cyber bullying, primarily occurring on social media but also present on various online platforms, is a prevalent issue in today's digital landscape, alongside data breaches. The emotional health, academic performance, and overall well-being of students can be adversely affected by cyber bullying.

According to Naveed et al. (2020), children who experience cyber bullying are at a higher risk of developing anxiety, feelings of despair, and reduced engagement in school activities. As a result, educators face significant pressure to address these challenges while maintaining a positive and secure learning environment. Another growing concern is identity theft, particularly among students, as they may not always be aware of how to protect their personal information while online. Unauthorised access to pupils' identities through phishing scams or compromised school systems can lead to significant financial or societal harm. Furthermore, educational institutions are increasingly becoming targets of ransomware attacks, which encrypt data and restrict access until a ransom is fulfilled. This greatly affects learning outcomes and results in financial losses for educational institutions.

Role of Teacher in Prevention of Cybercrime

The contribution of educators to the personal and academic development of their students is essential. It is essential to educate individuals on appropriate online conduct and to enhance awareness regarding the risks linked to internet usage for all stakeholders involved. Educators bear a significant responsibility in fostering information literacy. Educators ought to assist their students in assessing the reliability of information sourced from the internet. Instructors with expertise in technology are responsible for integrating digital tools into the curriculum while offering students the necessary resources and support. Through the guidance and support of students in practicing responsible and safe internet usage, educators can significantly aid in the battle against cybercrime. To enhance understanding of cyber security and the responsible use of internet resources, he may present students with case studies related to cybercrime and facilitate discussions on these subjects in the classroom. Students may be introduced to cybercrime and related terminology through the following methods: Introducing students to essential cyber security concepts: Introducing fundamental concepts

such as malware, phishing, social engineering, encryption, and secure communication could serve as an effective starting point for educators.

Presenting real-world examples and case studies. Utilising real-world examples and case studies can enhance students' comprehension of the tangible implications of cyber security risks and the potential consequences of negligence. Instructing on optimal cyber security practices: Educators hold a duty to educate their students about essential security practices that both individuals and organisations should implement. This includes the creation of strong passwords, the use of two-factor authentication, the importance of keeping software updated, and the necessity of avoiding unfamiliar or suspicious links and files. Educators may develop scenarios, assaults, and exercises related to cyber security, encompassing network scanning, incident response, and penetration testing. This provides students with the opportunity to acquire essential practical skills and engage in responding to real-life hazards. Educators should prioritise the importance of ethical conduct in cyber security, which includes refraining from unauthorised hacking, safeguarding user privacy, and promptly reporting security issues. Finally, to ensure that students receive precise and up-to-date information, educators must keep a close watch on developments and trends within the cyber security sector.

One way to do this is to enrol in continuing education courses, join relevant professional organisations, or attend relevant conferences. The fundamentals of copyright, including the kinds of works that are protected by it, the many kinds of creative common licenses, and what constitutes fair use of copyrighted content, may be covered by teachers. If students need help finding copyright-compliant materials for their work, they may provide them the names of places where they can locate it. The act of passing off another person's work as one's own is known as plagiarism, and teachers have the power to educate their pupils about this. Showing students how to properly credit others' work is a great way to help them become better writers. Open educational resources (OER), public domain works, and creative commons licensed content are some of the copyright friendly options that are trending right now. Teachers may help their students avoid violating owners' rights by informing them about these options. Teachers and parents or guardians may collaborate together to increase students' internet safety. It is possible to educate them on the topic of cybercrime and how to safeguard children by organising a variety of seminars, informative sessions, and chat sessions. Being vigilant against cybercrime is an essential part of our daily lives.

Considering that the cyber domain handles 80% of our tasks, doing so is essential. Even in the wee hours of the morning, we may research our zodiac signs, read the news, and send messages online. People check their messages and emails every 5 to 10 minutes to be informed about the latest happenings in our lives. In order to send out goodnight messages, we are online between the hours of 9 and 10. Greeting one another good morning and good night is the beginning and conclusion of our day. Everyone uses the internet for everything these days: shopping, studying, talking, and accounting. However, we are vulnerable to fraud, scams, phishing, and other forms of cybercrime when we do not take precautions. Cybercrime is a serious problem that needs our attention. The rise of cybercrime has made us all too conscious of how much easier life has become thanks to the internet. Cybercrime has permeated every aspect of our lives, and being informed via the internet is essential.

Conclusion

Everyone, from kids to adults, from teachers to students, from content creators to content consumers, is now involved in some kind of online activity. Some crimes, known as cybercrimes, are perpetrated due to the excessive usage of these activities. Now more than ever, we must educate the youth of today about the dangers of excessive use of social media and other internet tools like Instagram, WhatsApp, YouTube, Content Sharing App, and editing programs. The school's mission includes not only academic instruction but also the

dissemination of information on the responsible use of computers and the internet. Teachers should take the time to share their ideas and opinions on current technological developments, tools, and applications with their pupils since they are role models for them. While many are aware of cybercrime and its illicit character, not everyone has a thorough knowledge of the dangers posed by ransomware and similar attacks. You demonstrate an exceptional degree of cyber security awareness by being wary of utilising public Wi-Fi for important activities like online banking. The research also shows that there are some things people don't know, such how to spot phishing efforts and keep up with new cyber dangers. This highlights the need of continuous awareness and education programs to improve knowledge and readiness to combat cybercrime. With the digital world always changing and technology advancing at a quick pace, the study emphasises the crucial necessity of increasing teachers' understanding of cybercrime. The complexity of cybercrime, its forms, and the dangers connected with online activities are not well understood by educators, even if many of them have a rudimentary knowledge of cyber hazards. Educators must be able to recognise and avoid online risks in order to keep their pupils and themselves safe in today's technologically advanced and globally interdependent environment.

It's important to be aware of common cybercrime methods like phishing, ransomware, and identity theft. Being able to recognise suspicious online behaviour and safeguard personal information is key! It's really important to have comprehensive cyber security training and seminars designed for educators to help bridge this knowledge gap. In addition to raising awareness, these courses should offer participants practical steps to help them lower their risk of cybercrime, identify potential threats, and respond effectively to situations. One more way to ensure that everyone is continually learning and enhancing their cyber security skills is to incorporate it into regular teacher training programs. By providing teachers with the skills to navigate the internet safely, we not only protect them from potential dangers but also enable them to demonstrate safe online behaviour for their students. Educators can take the opportunity to enhance the safety of their schools for both students and staff by boosting their understanding of cybercrime. As educators, we should be knowledgeable about everything related to the internet. As educators, we have a wonderful responsibility to safeguard our children from cybercrime by considering these important aspects. So, let's encourage kids to be smart online to help them understand these cyber dangers better. It's important for everyone to feel confident that their personal information is safe on all social networking sites. It's really important to keep both students' and educators' accounts safe and secure.

Implications

There is a continuous relationship between the findings of any particular area of study and the applications that are used in the real world. These findings also have particular repercussions for students, parents, and administrators working in the field of education. Due to the fact that we are presently living in a cyber-era that is marked by globalisation and modernity, the research that is currently being conducted is more important than it has ever been before. Not only is the internet a need in the modern period, but it is also a method of promoting knowledge, learning, and interaction in many facets of life. This is because the internet is freely available to everyone. Inhaling, eating, and drinking are now all considered to be natural forms of consumption. Internet use as a means of escaping or easing the stressors that are associated with day-to-day existence. Notwithstanding this, there has been a significant increase in the amount of illegal behaviour that takes place inside the realm of online. In order for teenagers to have healthy lifestyles, they need to have instant access to tools that may modify their behaviour. The identification of problems at an early stage is the duty of a variety of individuals, including parents, teachers, counsellors, researchers, and peers. It is completely necessary to acknowledge the significance of the consequences that the present research has for the management of educational institutions. Modifications to the curriculum

of elementary, secondary and the higher education levels are required for effective educational policymaking.

For the purpose of raising awareness, it is suggested that children's books include a lesson or topic that focusses on cybercrime awareness. As a course or topic, cybercrime awareness needs to be introduced into the curriculum of diploma and bachelor's degree programs in education. The plain explanation for this is that the apprentice teachers will be the source of information for future generations. As soon as they recover consciousness, they immediately begin the process of teaching and raising awareness among their classmates, both inside the classroom and outside. Maintaining a connection to the internet is of utmost importance for teacher-in-training programs in both urban and rural areas. This is because it is essential for students to be motivated and inspired to achieve academic success, which in turn enables them to meet the expectations of society and successfully compete in the global marketplace. There is a possibility that educational programs on cyber security that are aired on television and radio are more likely to be successful in engaging youngsters and making them accessible.

References

Ahmed, Ali & Lundqvist, Karsten & Watterson, Craig & Baghaei, Nilufar. (2020). Teaching CyberSecurity for Distance Learners: A Reflective Study. 1-7. 10.1109/FIE44824.2020.9274062.

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

Archana Chanuvai Narahari and Vrajesh Shah (2016).Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand.

Bele (2014). Raising Awareness of Cybercrime-The Use of Education as a Means of Prevention and Protection. 10thInternational Conference Mobile Learning.

Chiua, W. Y., & Hob, H. F. (2019). Time to Educate the Educators: An Evaluation of Cyber Security Knowledge Awareness and Implementation for School Teachers in Taiwan. Proceedings of International Conference on Technology and Social Science

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cyber security: a systematic review of data availability. The Geneva Papers on Risk and Insurance-Issues and Practice, 1-39.

Duah F. (2013). Growing Global Threat of Cyber Crime: Implications for International Relations (Doctoral dissertation, University of Ghana), 2013. Retrieved online on the 11th of September 2018 from [http://ugspace.ug.edu.gh/bitstream/handle/123456789/5294/Francisca%20Duah_Growing%20Global%20Threat%20of%20Cyber%20Crime.%20Implications%20for%20In ternational%20Relations_2013.pdf?sequence=1]

Dwivedi and Bharati (2024). Challenges in Implementing Cyber Crime awareness Programs in Teacher Education, *Journal of Emerging Technologies and Innovative Research*, Volume 11, Issue 9, ISSN-2349-5162.

Jazeel, A., M. (2018). A Study on Awareness of Cyber crime among Teacher Trainees in Addalaichenai Government Teachers' College. *Journal of Social Welfare and Management, 10*(1), 31-34.

Ministry of Electronics & Information Technology. (2021). National Cyber Security Policy 2021. Government of India. Retrieved from https://www.meity.gov.in/

P Suvera & P R Tailor (2020). Cyber-crime awareness: a comparative study of male and female B.Ed. trainees. *International Journal of Indian Psychology*, 8(1), 361-365.

Prabu, P.S. (2015). Awareness on cyber crime among arts and science college students. *International Journal of Teacher Educational Research* (IJTER), 4(9), 7-13
Sulaiman, S &Sreeya, B (2019) Public awareness on cyber-crime with special reference to Chennai. *International Journal of Innovative and Exploring Engineering*, 9(1), 3362-3364. ISSN: 2278-3075.
The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, 1(2), 29–39.
The History of Cybercrime: A Comprehensive Guide (2021) (jigsawacademy.com)
Vinnarasi, L., & Nirmal Rajkumar, V. (2021). Awareness on Cyber Crime among B.Ed Students. *John Foundation Journal of EduSpark, 3*(4), 36-42.
Weru, Tracy & Sevilla, Joseph & Olukuru, John & Mutegi, Lorna & Mberi, Tabitha. (2017). Cybersmart children, cyber-safe teenagers: *Enhancing internet safety for children*. 1-8.