International Journal of Integrative Research (IJIR)
Vol.3, No.5, 2025: 329-342

Enhancing Cybersecurity Awareness through Training and Educational Programs for Schools and Colleges in Remuna Tehsil, Balasore District, Odisha

Satyajit Mahatab[1*], Ramesh Chandra Sahoo[2], Pankaj Kumar Dhal[3]
Fakir Mohan University, Balasore
Corresponding Author: Satyajit Mahatab; satyajitmahatabfmu@gmail.com

ARTICLEINFO

Keywords: Cybersecurity Awareness, Training Programs, Educational Initiatives, Mass Awareness, Digital Safety, Phishing Prevention

Received : 17, March
Revised : 24, April
Accepted: 30, May

ABSTRACT

In the contemporary digital landscape, the increasing integration of technology in educational and workplace settings has led to a heightened exposure to cyber risks. This study investigates the implementation of mass cybersecurity awareness initiatives through structured training and educational programs conducted across various schools, colleges, and workplaces in Remuna Tehsil, Balasore District, Odisha. The intervention targeted key educational institutions, including St. Thomas Convent School, Tundra High School, Saraswati Sishu Mandira, Bhimpura High School, Bhagabat Gosain High School, and several colleges, namely Rural Institute of Industrial Training Centres (Bhograi and Dehurda), Bahanaga College, Harekrushna Mahatab College, and Remuna Junior College. The objective was to enhance cybersecurity literacy among students & educators, equipping them with the essential knowledge to mitigate the risks of cyber threats such as phishing, malware, and data breaches. A multifaceted approach was employed, incorporating workshops, seminars, and hands-on activities to instill best practices for secure digital behavior and personal data protection. The findings highlight the significance of continuous, localized educational efforts in fostering a robust cybersecurity culture, emphasizing the critical need for proactive engagement in safeguarding digital environments. This paper discusses the methodologies used, the outcomes observed, and the implications for similar cybersecurity awareness programs in other regions

DOI: https://doi.org/10.59890/ijir.v3i5.25
E-ISSN 2988-2184
https://mrymultitechpublisher.my.id/index.php/ijir

INTRODUCTION

The Digital Transformation and Cybersecurity Challenges:

The rapid expansion of digital technologies has profoundly transformed how societies operate, offering new opportunities in education, business, healthcare, and governance. According to the International Telecommunication Union (ITU, 2020), over 4.9 billion people worldwide are now connected to the internet, which provides access to vast resources but also exposes individuals and institutions to increased cyber risks. As the digital world continues to evolve, cyberattacks have become a persistent threat, with devastating consequences for individuals, businesses, and even entire nations. The surge in cyber incidents, including ransomware attacks, data breaches, and phishing scams, highlights the urgent need for robust cybersecurity frameworks (Schneier, 2018).

While the increasing use of digital platforms has facilitated learning, collaboration, and innovation, it has also introduced new risks, especially within educational institutions. Schools, colleges, and universities, which hold valuable data such as academic records, personal information of students and staff, and intellectual property, have become prime targets for cybercriminals (Liu et al., 2019). According to the National Cyber Security Centre (NCSC, 2020), educational institutions are often seen as soft targets due to their inadequate cybersecurity infrastructure and the lack of awareness among students, staff, and teachers. These vulnerabilities can lead to severe consequences, including loss of sensitive data, identity theft, and disruption of academic activities.

India, with its rapidly growing digital economy, faces similar cybersecurity challenges. The Indian government's push towards digitalization through initiatives like Digital India and the National Mission on Education through Information and Communication Technology (NMEICT) has transformed the educational landscape (Sundararajan, 2019). However, despite the positive impacts of digitalization, the country has witnessed a rise in cybercrime, particularly in schools and colleges, where cybersecurity measures are often inadequate (Chawla, 2020). This growing threat necessitates the establishment of mass cybersecurity awareness programs to educate students & teachers about the risks associated with digital platforms and the best practices for securing personal and institutional data.

Cybersecurity Awareness in Educational Institutions:

Educational institutions have become increasingly dependent on digital platforms for teaching, administration, and student interaction. This widespread adoption of technology, however, has made these institutions more vulnerable to cyber threats. Research by Johnson et al. (2018) shows that a large proportion of cyberattacks in schools and colleges are driven by human error, such as falling victim to phishing scams or failing to secure sensitive data. Moreover, many educational institutions in India, particularly those in rural areas like Remuna Tehsil in Odisha, lack the necessary infrastructure to address these vulnerabilities, leaving them exposed to cyberattacks (Goswami, 2020).

While cybersecurity education is critical in all sectors, it is especially crucial in schools and colleges, where students are the primary users of digital tools but often lack the knowledge to protect themselves. Studies by Agarwal and Sharma (2021) have shown that students are particularly vulnerable to cyber threats because they are less likely to recognize phishing attempts or understand the importance of password security. Furthermore, educational staff, who may not have received formal training in cybersecurity, are often unaware of the threats posed by their own online behavior, such as using weak passwords or failing to recognize malicious emails (Desai et al., 2019).

Cybersecurity awareness programs in educational institutions must go beyond teaching general internet safety. According to Saini (2020), effective cybersecurity training should involve practical lessons on identifying and avoiding cyber threats, using secure online tools, and understanding the importance of data privacy. These programs should be integrated into the curriculum and extended to all levels of education, from primary schools to higher education institutions, to ensure that students and educators are well-prepared to navigate the digital world securely (Patel & Agarwal, 2021).

Cybersecurity Awareness in Remuna Tehsil:

Remuna Tehsil, located in the Balasore District of Odisha, is home to several educational institutions and workplaces that could greatly benefit from cybersecurity awareness programs. The region, while growing in terms of digital infrastructure, faces significant challenges related to internet connectivity, digital literacy, and cybersecurity education. Schools in Remuna, such as St. Thomas Convent School, Tundra High School, and Saraswati Sishu Mandira, have begun integrating digital tools into their classrooms but lack comprehensive cybersecurity training for students and teachers. Colleges such as Bahanaga College and Harekrushna Mahatab College are also increasingly adopting digital technologies for administration and education, but their staff and students often remain ill-equipped to recognize and counteract cyber threats.

The need for mass cybersecurity awareness programs in Remuna Tehsil is further emphasized by the lack of specialized cybersecurity professionals in the region. As reported by Gupta et al. (2020), rural areas in India often struggle with a shortage of trained IT professionals who can implement robust cybersecurity measures. In the absence of such expertise, educational and workplace cybersecurity programs must be designed and delivered by external experts or through collaboration with government and non-government organizations specializing in digital literacy and security.

Challenges to Effective Cybersecurity Awareness:

Despite the clear need for cybersecurity awareness programs, there are significant challenges to their effective implementation. First, the lack of infrastructure in rural schools and colleges presents a barrier to training programs. Many schools in Remuna Tehsil lack the necessary computer labs, internet connectivity, and up-to-date software to conduct comprehensive cybersecurity education (Sundararajan, 2020). Additionally, many teachers and school staff members do not have the technical knowledge required to teach cybersecurity concepts, making it difficult to integrate such training into the existing curriculum (Chawla, 2021).

Another challenge is the reluctance of students to engage with cybersecurity training programs. Studies by Kumar (2019) and Saini (2020) indicate that many students perceive cybersecurity education as either irrelevant to their daily lives or too complex to comprehend. Similarly, students in rural areas may view cybersecurity training as an unnecessary task that distracts from their primary job duties (Patel & Agarwal, 2021). Overcoming this reluctance requires designing engaging, interactive, and accessible cybersecurity training that demonstrates the real-world importance of online safety.

Finally, the evolving nature of cyber threats presents an ongoing challenge. Cybercriminals constantly develop new methods of attack, making it difficult for training programs to stay current. Researchers such as Verma (2020) suggest that cybersecurity training programs should be continuously updated to reflect the latest threats and trends, ensuring that participants are always equipped with the most relevant knowledge.

Purpose of the Study:

This study aims to examine the effectiveness of mass cybersecurity awareness programs implemented in schools & colleges within Remuna Tehsil, Balasore District, Odisha. The primary goal is to evaluate the level of cybersecurity awareness among students & teachers before and after the implementation of these programs. The study also seeks to identify the challenges faced in delivering these programs and the strategies employed to overcome them. By providing training sessions and workshops, this research will contribute to the development of a scalable model for cybersecurity education that can be replicated in other rural regions of India. The findings will help inform policy recommendations for integrating cybersecurity training into school and college curricula and workplace training programs.

As the digital landscape continues to evolve, cybersecurity education has become an essential aspect of ensuring safe online practices. This study, focusing on the implementation of cybersecurity awareness programs in Remuna Tehsil, will provide critical insights into the challenges and successes of such initiatives in rural India. The research aims to foster a culture of cybersecurity literacy in schools, colleges, and workplaces, empowering individuals to protect themselves and their data from the growing range of cyber threats. By addressing the gaps in cybersecurity knowledge and providing practical training, this initiative has the potential to significantly reduce the risk of cyberattacks in the region and beyond.

LITERATURE REVIEW

The increasing integration of digital technologies into everyday life, especially in educational institutions and workplaces, has made cybersecurity a critical concern. Cybersecurity, traditionally a specialized field, has now become a subject of general concern as every digital interaction presents a potential risk. The term "cybersecurity awareness" refers to the understanding and proactive attitude of individuals regarding the risks posed by cyber threats, as well as the knowledge of practices that can help mitigate these risks. According to studies by Schneier (2018) and Liu et al. (2019), the ability of individuals to recognize and defend against cyber threats, such as phishing and malware, is essential for building a culture of cybersecurity in educational and organizational settings.

Cybersecurity awareness programs are critical in helping individuals navigate the online environment securely. In India, the importance of such programs is highlighted by the increasing number of cyberattacks targeting educational institutions and businesses. The National Cyber Security Centre (NCSC, 2020) reported a significant rise in cyber incidents, with educational institutions being particularly vulnerable due to a lack of cybersecurity infrastructure and the abundance of sensitive data they hold. As digital technology continues to pervade all aspects of life, cybersecurity awareness must be a priority for all stakeholders, including students, teachers, and management.

Cybersecurity Threats in Educational Institutions

Educational institutions, including schools, colleges, and universities, are increasingly becoming targets for cyberattacks due to the vast amount of personal and academic data they hold (Chawla, 2020). The vulnerability of educational institutions is further exacerbated by the lack of adequate cybersecurity measures and a general lack of awareness among students and staff (Sundararajan, 2019). According to a study by Jain et al. (2021), cyberattacks such as phishing, data breaches, and ransomware have become prevalent in schools and colleges, primarily due to human error. Educational staff often fail to implement proper cybersecurity measures, while students may be unaware of the risks they face in online environments.

Cyberattacks in educational institutions not only compromise personal and academic data but also disrupt academic activities, hindering learning outcomes and damaging the reputation of educational establishments. The Indian government's Digital India initiative, which aims to increase the use of technology in education, has raised concerns regarding the cybersecurity preparedness of schools and colleges (Agarwal & Sharma, 2021). Despite the rapid digital transformation, many educational institutions in rural areas, including Remuna Tehsil, face significant challenges in implementing robust cybersecurity measures.

In their study, Agarwal and Sharma (2021) emphasized the need to integrate cybersecurity education into the school curriculum to address these gaps. By providing students with a foundational understanding of cyber threats and mitigation strategies, educational institutions can better prepare their students to recognize and avoid common risks. Furthermore, educators must also be educated on the importance of cybersecurity, as their failure to adopt secure practices can put entire school systems at risk (Chawla, 2020).

Human Error and Cybersecurity Vulnerabilities:

Human error is the primary cause of cybersecurity breaches in educational institutions and workplaces. According to a report by Verizon (2020), over 60% of cyberattacks are caused by human mistakes, such as opening phishing emails, failing to implement secure password policies, or mishandling sensitive data. Research by Liu et al. (2019) also found that a lack of awareness about cybersecurity best practices makes individuals susceptible to falling victim to attacks. In schools, colleges, and workplaces, students may not understand the full scope of the cyber threats they face, leading them to unknowingly engage in risky behaviors. For instance, using weak passwords or failing to recognize phishing emails can result in substantial data breaches and financial losses.

The role of cybersecurity training and awareness in mitigating human error cannot be overstated. In a study by Saini (2020), the author emphasized that effective training programs could reduce human error-related cyber incidents significantly. Programs that incorporate real-world scenarios, such as simulated phishing exercises, can help individuals identify and avoid cyber threats. These practical exercises can also help reduce the overall risk within an organization or educational institution by improving the decision-making skills of students when interacting with digital tools.

Cybersecurity Training Programs and Their Effectiveness:

Cybersecurity awareness programs have proven to be effective in improving knowledge about online risks and changing behavior. Studies by Patel and Agarwal (2021) have shown that integrating cybersecurity awareness into educational curricula has a long-term positive effect on students' ability to identify cyber threats. Furthermore, research by Gupta et al. (2020) indicates that when students are taught cybersecurity fundamentals, they are more likely to adopt secure practices in both their academic and personal digital interactions.

In the workplace, continuous cybersecurity training programs can significantly reduce the likelihood of successful cyberattacks. According to the Center for Internet Security (CIS, 2020), organizations that implement cybersecurity training programs see fewer incidents related to human error. Simulated phishing exercises, regular workshops, and providing updates on the latest cyber threats have been shown to help students recognize and respond to security risks more effectively. Tiwari (2021) highlights the importance of integrating cybersecurity awareness into regular training schedules to maintain a high level of vigilance among students, especially in sectors that deal with sensitive or classified information, such as healthcare and finance.

In the context of schools and colleges in rural areas, such as Remuna Tehsil, training programs must be specifically designed to cater to the needs of these institutions. Research by Saini (2020) suggests that rural institutions often lack the infrastructure and expertise to deliver effective cybersecurity training. Therefore, partnerships with government organizations, non-profits, and private-sector companies that specialize in cybersecurity could provide the necessary resources to implement these programs effectively.

Challenges to Cybersecurity Awareness in Rural Areas:

Implementing cybersecurity awareness programs in rural areas presents several unique challenges. First, there is often a lack of infrastructure, including reliable internet access and up-to-date computers, which makes it difficult for educational institutions to adopt and teach cybersecurity practices (Goswami, 2020). According to Kumar (2019), rural schools and colleges in India, including those in Remuna Tehsil, frequently operate with limited resources, which can hinder their ability to implement training programs. Additionally, teachers and staff in rural schools often lack the technical expertise required to teach complex cybersecurity concepts effectively.

Another challenge is the limited interest or perceived relevance of cybersecurity training among students in rural areas. Many individuals, especially in non-urban settings, may not fully understand the risks associated with online activities and may perceive cybersecurity as a distant concern that does not impact their daily lives (Patel & Agarwal, 2021). Overcoming this mindset requires creating engaging and practical training programs that demonstrate the real-world implications of cyber threats. Research by Chawla (2020) indicates that using case studies of local cyber incidents or examples of personal data breaches can help contextualize the importance of cybersecurity for individuals in rural areas.

Moreover, the rapidly evolving nature of cyber threats poses an ongoing challenge to cybersecurity awareness programs. As cybercriminals continually develop new tactics and tools, it is essential that training programs remain up-to-date to ensure that participants are equipped to defend against the latest threats (Verizon, 2020). Studies by Desai et al. (2019) suggest that regular updates to training materials, as well as ongoing cybersecurity education, are necessary to address the dynamic nature of the threat landscape.

Role of Government and Non-Governmental Organizations in Cybersecurity Awareness:

Government and non-governmental organizations play a crucial role in promoting cybersecurity awareness, especially in rural areas. Initiatives like the Digital India campaign and the National Mission on Education through Information and Communication Technology (NMEICT) aim to bring digital literacy to rural populations. According to Sundararajan (2020), these initiatives must include a strong focus on cybersecurity to ensure that individuals in rural India are not left vulnerable to cyber threats. Government partnerships with educational institutions and NGOs can provide the necessary infrastructure, resources, and expertise to implement cybersecurity training programs in rural areas.

Non-governmental organizations (NGOs) and industry experts can also assist in delivering cybersecurity training through workshops, online courses, and awareness campaigns tailored to the needs of rural communities. In fact, many NGOs are already working to address this gap. The Cyber Peace Foundation, for example, conducts training programs in schools and colleges across India to raise awareness about online threats and data protection (Cyber Peace Foundation, 2021).

The literature reviewed highlights the growing importance of cybersecurity awareness in educational institutions, workplaces, and rural areas. Cybersecurity awareness programs have proven to be effective in reducing the risks posed by cyber threats by educating students & teachers about best practices for online safety. However, several challenges remain, particularly in rural areas like Remuna Tehsil, where limited infrastructure and resources hinder the effectiveness of cybersecurity training initiatives. This literature review suggests that comprehensive, targeted, and continuously updated cybersecurity awareness programs are essential for reducing vulnerabilities in both educational and organizational contexts. Further research is needed to explore the impact of such programs in rural settings and to develop scalable models for integrating cybersecurity education into existing curricula and workplace training programs

METHODOLOGY

The primary target audience for this study consists of students and teachers from various schools and colleges in Remuna Tehsil, Balasore District, Odisha. This region has witnessed a steady rise in the adoption of digital technologies in educational settings, making it essential to equip students and staff with the knowledge and skills to navigate the digital landscape securely. Schools such as St. Thomas Convent School, Tundra High School, Saraswati Sishu Mandira, Bhimpura High School, and Bhagabat Gosain High School, as well as colleges including Bahanaga College, Harekrushna Mahatab College, and Remuna Junior College, are the key institutions targeted in this study. The focus on these institutions is critical as students and teachers are frequently exposed to online platforms for educational purposes but may lack awareness about cybersecurity threats.

Data collection will involve both quantitative and qualitative methods to provide a comprehensive assessment of the current level of cybersecurity awareness among the participants. To gather baseline data, a structured questionnaire will be administered to students and teachers before the implementation of the cybersecurity awareness programs. The survey will assess participants' current knowledge, behaviors, and perceptions regarding cybersecurity risks and safe online practices. Key areas of focus will include awareness of common cyber threats, such as phishing, malware, and identity theft, as well as practices related to password security, the use of secure websites, and the sharing of personal information online. Additionally, semi-structured interviews will be conducted with a subset of participants from each institution to gain deeper insights into their understanding of cybersecurity and any challenges they have encountered related to online safety.

After the training sessions are completed, a follow-up survey will be distributed to assess any changes in participants' cybersecurity awareness and behavior. The post-training questionnaire will mirror the pre-training survey to measure the effectiveness of the program in increasing knowledge and changing practices. This comparison will help determine whether the training has had a tangible impact on participants’ ability to recognize and respond to cybersecurity threats. Furthermore, focus group discussions will be organized with students and teachers to discuss their experiences with the training program, gather feedback, and identify areas for improvement.

The data collected from these surveys and interviews will be analyzed using a mixed-methods approach. The quantitative data from the pre- and post-training surveys will be analyzed using descriptive statistics, such as mean scores, frequency distributions, and percentage changes, to evaluate the impact of the training program. The qualitative data from interviews and focus group discussions will undergo thematic analysis to identify recurring themes, such as common challenges faced by participants, feedback on the training methods, and perceptions regarding the relevance and applicability of the program. This analysis will provide deeper insights into the factors that contribute to the success or failure of cybersecurity awareness initiatives.

The study will also address the ethical considerations associated with data collection. All participants will be informed about the purpose of the study and will be asked to provide their consent before participating. Anonymity and confidentiality will be maintained throughout the research process, and participants will have the option to withdraw from the study at any time without any consequences. The findings from this study will be aggregated and presented in a way that ensures the privacy of all participants.

This methodology will allow for a comprehensive evaluation of the cybersecurity awareness programs in schools and colleges in Remuna Tehsil. By collecting both quantitative and qualitative data, the study aims to provide a detailed understanding of how such programs influence students' and teachers' knowledge, attitudes, and behaviours regarding cybersecurity. The insights gained from this research can inform future cybersecurity initiatives in educational settings and help create more effective training programs tailored to the specific needs of rural schools and colleges in India.

RESULTS AND DISCUSSION

The study revealed several key findings that highlight the current state of cybersecurity awareness in Remuna Tehsil, Balasore District. A primary observation was the low level of awareness and knowledge about cybersecurity and the social determinants of security among the community members in Remuna. This lack of understanding points to a critical need for more comprehensive educational programs focused on cybersecurity, especially regarding the risks and threats that exist in the digital world.

One of the most notable concerns expressed by participants was cyber hacking in the banking sector. A strong sense prevailed among the participants that cyberattacks targeting the banking sector are a significant issue for their communities. This concern suggests a heightened vulnerability to financial cybercrimes, and underscores the urgent need for awareness programs that teach secure online banking practices, such as identifying phishing attempts and securing financial transactions online.

Another key finding was the lack of information and resources available at the community level. Many individuals in Remuna Tehsil have limited access to reliable cybersecurity resources and do not have sufficient knowledge of the tools and practices needed to secure personal and institutional data. This gap in resources points to the necessity of making cybersecurity information more accessible to the community through local workshops, printed materials, and digital platforms.

Participants also expressed a strong need for more information on the prevention and management of IT/cybersecurity risks. There was a clear demand for programs that educate individuals about the risk factors associated with cybersecurity threats and teach practical strategies to mitigate these risks. This need for greater knowledge about prevention and management emphasizes the importance of cybersecurity education as a preventive measure against the growing number of cyberattacks.

The study identified several educational and awareness strategies for potential implementation in Remuna. These strategies focus on the style, format, content, and language preferences for educational materials, ensuring that the information is accessible and engaging. Participants suggested that cybersecurity education materials be culturally relevant, easy to understand, and use simple language. Additionally, there was a preference for interactive learning methods that could help reinforce cybersecurity concepts in a more engaging way.

A community outreach and engagement model were developed based on the study's findings. This model aims to integrate cybersecurity awareness into the community by utilizing existing structures such as local schools, colleges, and community centers. It is built on the cybersecurity framework and strategies, focusing on continuous engagement through workshops, seminars, and collaboration with local authorities and organizations.

The study also found that there were differences in cybersecurity literacy between college students and school pupils. College students showed a significantly higher level of cyber literacy due to the comparative IT richness of their institutions, where digital resources and access to technology are more readily available. However, the study found that school pupils in Remuna displayed very poor knowledge of cybersecurity, largely because of lack of information and technological support in the schools. This points to a need for schools to enhance their IT infrastructure and provide more targeted cybersecurity education.

Regarding IT knowledge among college students, about 74% of students in the study were found to have some form of IT knowledge, primarily due to their interactions with the internet and digital platforms. However, their understanding of cybersecurity remained superficial, focused on basic digital skills rather than secure online behaviour, which calls for more specialized cybersecurity training.

Finally, a significant portion of school students, only 8%, reported involvement in IT or cybersecurity knowledge through government-led initiatives, such as computer education programs at the school level. This indicates that cybersecurity education is still not adequately integrated into the school curriculum, particularly in rural areas like Remuna Tehsil, where government initiatives need to be scaled and expanded to reach a wider student base.

These findings underscore the urgent need for targeted cybersecurity awareness programs in Remuna Tehsil, specifically tailored to address the gaps in knowledge, infrastructure, and resources among the community. The results highlight the importance of improving digital literacy and cybersecurity education, particularly among school students, and ensuring that information is easily accessible, culturally relevant, and practical for the local population.

CONCLUSIONS AND RECOMMENDATIONS

Recommendations

Based on the key findings of the study, several recommended solutions are proposed to address the gaps in cybersecurity awareness and education in Remuna Tehsil. These solutions focus on improving the knowledge and skills of the community, particularly students and teachers, in securing their digital environments. The first recommendation is the integration of cybersecurity education into the school curriculum. Schools in Remuna, such as St. Thomas Convent School, Tundra High School, Saraswati Sishu Mandira, and others, should include basic cybersecurity concepts in their educational programs. This curriculum should cover essential topics such as recognizing common cyber threats (e.g., phishing, malware), understanding password management, and practicing secure online behavior. Since many students have limited awareness of cybersecurity, it is crucial that the curriculum is interactive and age-appropriate, incorporating practical lessons such as how to identify suspicious emails or secure their personal devices.

In addition to the curriculum, targeted cybersecurity workshops should be organized for college students at institutions like Bahanaga College, Harekrushna Mahatab College, and Remuna Junior College. These workshops can go beyond the basics to address more complex issues, such as data breaches, ransomware, and financial cybercrimes, which are relevant to their digital lives. Hands-on sessions should be included to allow students to practice real-world scenarios like identifying phishing attempts or securing social media accounts. As college students are more exposed to digital platforms and online resources, these workshops can be tailored to fit their needs and provide them with the necessary skills to navigate the digital space securely.

A critical issue identified in the study is the lack of information and resources available at the community level. To address this, collaboration with government agencies and NGOs is essential to make cybersecurity resources more accessible. These organizations can help produce and distribute materials such as brochures, pamphlets, and posters in local languages, which explain the basics of online safety and data protection. Online resources, including videos and infographics, can be made available on dedicated platforms to ensure easy access for the local population. These resources can be shared across schools, community centers, and local businesses to reach a wide audience and promote secure online practices.

Moreover, a community outreach and engagement model should be developed, focusing on involving local leaders and educators in spreading cybersecurity awareness. The model should include localized workshops and seminars, where local experts or cybersecurity professionals can educate the community about common cyber threats and best practices for protecting personal and institutional data. The community outreach model can be enhanced by leveraging existing structures, such as local schools and community centers, which can act as hubs for cybersecurity education and awareness campaigns. Additionally, local leaders, including teachers, village heads, and NGO workers, should be trained as cybersecurity ambassadors, empowering them to educate others and create a sustainable, community-driven cybersecurity culture.

In addition to formal education and community outreach, the study recommends incorporating interactive and gamified learning approaches to engage students and teachers more effectively. Cybersecurity literacy can be enhanced through gamified quizzes, escape room challenges, and online competitions that involve identifying cyber threats or solving cybersecurity-related puzzles. These activities can make learning about cybersecurity more fun and engaging, especially for younger students. Offering digital badges or certificates for completing cybersecurity challenges can also motivate participants to continue their education in this field. This interactive approach can help students and educators retain the knowledge while applying it to real-life situations.

The study also highlights the need for train-the-trainer programs, where select educators are trained extensively in cybersecurity practices and then act as trainers for other teachers and students. These programs would help increase the overall cybersecurity knowledge among educators, ensuring that they are equipped to teach their students about online risks and how to mitigate them. As many teachers in rural areas lack technical expertise, such programs are vital for ensuring that cybersecurity education becomes an integral part of the teaching process. Teachers, once trained, can pass on this knowledge to students, creating a cybersecurity-conscious educational environment.

Finally, establishing a local cybersecurity task force composed of representatives from local schools, colleges, businesses, and community organizations would help ensure the effective implementation of cybersecurity initiatives. This task force would be responsible for continuously evaluating the success of awareness programs, monitoring the emergence of new cyber threats, and updating educational materials to reflect the latest cybersecurity trends. The task force could also collaborate with external cybersecurity experts to bring in additional expertise and ensure that the community receives the most up-to-date information and resources.

These recommendations aim to create a cyber-aware community in Remuna Tehsil by focusing on comprehensive educational strategies, community engagement, and the development of practical tools and resources. By implementing these solutions, Remuna Tehsil can enhance cybersecurity literacy and empower students, teachers, and the broader community to take proactive steps in securing their digital lives.

Conclusion

In conclusion, the study highlights the pressing need for improved cybersecurity awareness and education in Remuna Tehsil, especially within the educational sector. The findings demonstrate a significant gap in cybersecurity knowledge among school students, with only 74% of college students possessing some IT knowledge, and a mere 8% of school students being exposed to IT education through government programs. This highlights the lack of adequate cybersecurity training at the school level, particularly in rural areas. Additionally, the study emphasizes the growing concern around cybersecurity threats, particularly in the banking sector, and the need for increased preventive measures and management strategies within the community.

The recommendations provided aim to address these gaps by integrating cybersecurity education into school curricula, conducting targeted workshops for college students, and improving community outreach and engagement. By equipping students and educators with the necessary knowledge and tools, Remuna Tehsil can foster a culture of cybersecurity awareness, reducing vulnerabilities and empowering individuals to protect their digital lives. Through collaboration with governmental bodies, NGOs, and local community leaders, it is possible to implement these solutions effectively and sustainably, ensuring that the entire community is well-prepared to face the evolving digital threats. The successful implementation of these strategies will not only improve cybersecurity awareness but will also help safeguard personal and institutional data, ultimately enhancing the security and resilience of Remuna Tehsil in the digital age.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Directorate of Distance & Continuing Education (DDCE), Fakir Mohan University, Balasore, Odisha–756020, for providing academic support and necessary resources for this study. We also extend our thanks to the educational institutions in Remuna Tehsil, Balasore District, for their cooperation and participation. Special appreciation is due to our colleagues Mr. Ramesh Chandra Sahoo and Mr. Pankaj Kumar Dhal for their valuable contributions to this research.

REFERENCES

Agarwal, R., & Sharma, S. (2021). Cybersecurity Education and Its Impact on Indian Students: Challenges and Solutions. International Journal of Information Security, 16(1), 45-56.

Center for Internet Security (CIS). (2020). 2020 Cybersecurity Best Practices for Small and Medium-Sized Businesses. https://www.cisecurity.org

Chawla, S. (2020). Cybersecurity in Rural India: Addressing the Challenges in Educational Institutions. Journal of Cybersecurity, 10(3), 189-205.

Desai, R., Sharma, K., & Saini, P. (2019). Cybersecurity Training Programs and Their Effectiveness in Schools and Colleges. Journal of Educational Technology, 18(4), 305-319.

Goswami, A. (2020). Cybersecurity Challenges in Rural Educational Institutions in India. International Journal of Cybersecurity and Education, 8(2), 101-113.

Gupta, R., Kumar, S., & Sharma, N. (2020). Cybersecurity Infrastructure in Rural India: A Review of Challenges and Opportunities. Indian Journal of Cybersecurity, 12(1), 87-95.

Jain, P., Mehta, A., & Agarwal, R. (2021). Building a Cybersecurity Culture in Schools: A Case Study of Awareness Programs in India. Journal of Cybersecurity Education, 9(2), 114-125.

Johnson, M., Smith, D., & Thomas, R. (2018). Cybersecurity Education: Bridging the Awareness Gap. International Journal of Information Security, 15(3), 167-182.

Kumar, R. (2019). Cybersecurity Awareness in Rural India: A Case Study of Remuna Tehsil. Journal of Information Security, 13(1), 45-58.

Liu, X., Zhang, Y., & Li, J. (2019). Cybersecurity Threats in Educational Institutions: A Global Perspective. International Journal of Cybersecurity, 14(4), 256-267.

Patel, S., & Agarwal, A. (2021). Building Cybersecurity Literacy in Rural India: Key Strategies for Success. Journal of Rural Education, 5(3), 211-225.

Saini, R. (2020). Cybersecurity in Education: Importance and Implementation Challenges. International Journal of Educational Technology, 12(4), 201-215.

Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W.W. Norton & Company.

Sundararajan, V. (2019). Digital India and Cybersecurity: A Policy Perspective. Journal of Information Security and Privacy, 11(2), 98-111.

Tiwari, A. (2021). Workplace Cybersecurity: A Strategic Approach for Mitigating Risks. Journal of Cybersecurity Management, 7(2), 99-112.

Verizon. (2020). 2020 Data Breach Investigations Report. https://www.verizon.com

World Economic Forum. (2021). The Global Risks Report 2021. https://www.weforum.org