Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2021 = 7.380, www.srjis.com
PEER REVIEWED & REFEREED JOURNAL, NOV-DEC, 2022, VOL- 10/74

BEHAVIOURAL SHIFTS IN CYBERSECURITY: A STUDY OF TRAINING PROGRAMME EFFECTIVENESS

Dr. Sheetal M. Zalte

Associate Professor, Smt. Kapila Khandvala College of Education (Autonomous), Santacruz, Mumbai

Paper Received On: 20 November 2022

Peer Reviewed On: 10 December 2022

Published On: 01 January 2023

Abstract

In an age marked by rapid technological advancement, the escalating threat of cyber fraud poses significant challenges across diverse sectors, necessitating robust cybersecurity measures. This research paper explores the effectiveness of a cybersecurity training program for student teachers, aiming to enhance their knowledge, awareness, attitude, and practices related to cybersecurity. Against the backdrop of staggering global cybercrime costs, the study acknowledges the dual perspective of this issue, both as a global and local concern.

The literature review highlights the intricate relationship between technology, education, and cybersecurity, emphasizing the need for educators to navigate the complexities of the digital landscape. Recognizing the vulnerability of students in the virtual space, the study focuses on student teachers as agents of change, aiming to equip them with skills to fortify the digital defences of future generations. The research methodology employs a quantitative approach, utilizing one-group pre-test-post-test design. The study includes fifty student teachers enrolled in a B.Ed. program, assessing the effectiveness of a thirty-hour cybersecurity literacy programme. Results indicate a significant improvement in student teachers' cybersecurity knowledge, awareness, attitude, and practices post-training, emphasizing the effectiveness of the intervention.

Correlation analysis reveals strong relationships among different aspects of cybersecurity literacy, highlighting the interconnected nature of knowledge, awareness, attitude, and practices. The study advocates for the integration of cybersecurity education into formal teacher education programmes and emphasizes the importance of continuous professional development to address evolving cyber threats.

The research contributes to building a secure digital learning environment and emphasizes the need for ongoing interventions to adapt to the ever-changing cybersecurity landscape.

Keywords: *student teachers, cybersecurity literacy, teacher education, training programme, digital learning environment.*

Introduction: In an era dominated by rapid technological advancements, the pervasive threat of cyber fraud is a big problem, infiltrating diverse sectors and causing unprecedented damage. Hacking into crucial and confidential information, whether from governmental or non-governmental organizations, has escalated to alarming proportions. The magnitude of the financial losses and the consequential misuse of vital information highlight the pressing need for robust cybersecurity measures across all facets of society.

Global cybercrime costs a staggering $6 trillion annually, representing 0.8% of the world's GDP (Source: Cybersecurity Ventures). Ransomware attacks alone cost businesses $46 billion in 2021, a 69% increase from 2020 (Source: Palo Alto Networks). A 2021 report by the Government Accountability Office (GAO) found that federal agencies experienced almost $139 billion in financial losses from cyberattacks between 2016 and 2020. The impact of cybercrime is not confined to international borders alone; it is a pressing local issue as well. The NASSCOM-DSCI Report published in December 2021, estimated cybercrime cost the Indian economy a staggering $93 billion in 2021. While this report does not explicitly break down the figure for cyber-attacks, it emphasizes the substantial economic toll that cyber threats pose at the national level. This dual perspective, both global and local, reinforces the urgency of addressing cybersecurity challenges comprehensively, acknowledging the widespread implications of this evolving threat landscape.

Governmental bodies, entrusted with safeguarding sensitive data, find themselves grappling with increasingly sophisticated cyber-attacks, resulting in huge financial losses and compromising national security. Simultaneously, non-governmental organizations, repositories of valuable information, face similar threats that extend beyond monetary concerns, impacting the very fabric of societal trust.

Against this backdrop, the imperative for cybersecurity training becomes abundantly clear, particularly at the foundational level of education. School-level training emerges as a crucial line of defence against the rising tide of cyber threats, with teachers assuming the role of agents of change. These educators, who guide and mould the future generations, play a pivotal role in equipping students with the skills necessary to navigate the complex and evolving landscape of cyber threats. By instilling a robust understanding of cybersecurity principles, teachers become instrumental in fostering a generation that is not only aware of the risks but also empowered to proactively protect themselves and society from the dangers of cyber fraud. This interconnected narrative underlines the urgency of integrating cybersecurity education into the very fabric of our educational systems, ensuring that the agents of change—our teachers—are well-equipped to fortify the digital defenses of the generations they nurture.

Teachers lead change, cultivating cybersecurity awareness and resilience in students, contributing to a secure digital space.

The inexorable integration of technology into educational frameworks, exemplified by the Digital India programme, has catapulted the traditional paradigm of teaching into an era marked by virtual connectivity and unprecedented opportunities. The recent global pandemic has not only accelerated this digital transformation but has also underscored the imperative for educators to adeptly navigate the virtual landscape. This transition, while offering convenience, has brought to the forefront the latent vulnerabilities of the virtual world, particularly within the realm of education. Educators, entrusted with the responsibility of guiding and safeguarding students, suddenly found themselves navigating uncharted territories in the cyber space. Recognizing the vulnerability of students in this virtual space, it became essential to equip educators with the necessary skills to protect their students effectively. However, the stark reality revealed a significant gap in the preparedness of teachers for these new challenges. This paper aims to explore the efficacy of a cybersecurity training programme designed for student teachers in addressing the emerging challenges within this dynamic educational landscape.

Aim of the Study The study aims to assess the effectiveness of a cybersecurity training programme designed for student teachers in enhancing their knowledge, awareness, attitude, and practices related to cybersecurity. The study seeks to determine the effectiveness of the training programme on the preparedness of future educators in navigating the challenges of the digital environment and safeguarding students in the virtual space.

Objectives

1. To design a programme on cybersecurity for student teachers.
2. To study the perceived effectiveness of the training programme on different aspects of cybersecurity literacy, such as knowledge, awareness, attitude, and practices.
3. To study the correlations between different aspects of cybersecurity literacy, such as knowledge, awareness, attitude, and practices.

Null Hypothesis (Ho):

- (Ho1) There is no significant difference between the mean scores of Pre-test and Post-test for each of the aspects (knowledge, awareness, attitude, and practices) and aggregate.
- (Ho2) There is no significant correlation among the four aspects of cybersecurity literacy.

Literature Review

Technology, Education, and Cybersecurity: An Interwoven Landscape: The rise of digital technologies in education sparks a crucial conversation about cybersecurity. Johnson et al. (2015) and Bates (2016) highlight the transformative impact of technology on education, urging educators to navigate both the possibilities and pitfalls of online pedagogy. Bates (2016) particularly cautions against potential risks like cybersecurity threats and student privacy concerns, setting the stage for a multifaceted examination of challenges in the digital learning environment.

Teacher Preparedness and the Technological Pedagogical Content Gap: Koehler and Mishra (2009) advocate for integrating Technological Pedagogical Content Knowledge (TPACK) into teacher education to address the complexities of digital teaching. However, Ertmer et al. (2012) reveal ongoing gaps in teachers' technology proficiency, especially concerning cybersecurity. This dissonance between the desired integration of TPACK and actual teacher preparedness points to a critical area for intervention in teacher education programmes.

Ethical Considerations in Online Education: Selwyn (2017) and Crosslin et al. (2017) shed light on ethical issues within online education, emphasizing educators' responsibility in mitigating cyberbullying, digital harassment, and unauthorized platform access. Their analysis underlines the need for clear guidelines and ethical frameworks within online learning environments.

Cybersecurity Literacy and Education: Equipping Educators and Students: Rezai and Salehahmadi (2019) advocate for incorporating cybersecurity education into formal teacher education programmes. This aligns with the broader theme of the literature, emphasizing the crucial role of cybersecurity-literate educators in guiding students through the virtual world. Mancuso's (2020) exploration of cybersecurity challenges faced by educational institutions further highlights the vulnerability of these settings and the need for proactive measures to safeguard sensitive data and maintain secure learning environments.

Understanding KAAP for Effective Cybersecurity Education: The success of cybersecurity education hinges on understanding individuals' knowledge, awareness, attitude, and practices (KAAP). Recent studies (Dwivedi et al., 2021) shed light on knowledge gaps in various demographics and professions. Research on awareness (Acar et al., 2021; Marwan et al., 2020) highlights the effectiveness of targeted campaigns in specific contexts, while also revealing challenges in maintaining long-term awareness and adapting to evolving threats. Studies on attitude (Graeber et al., 2019; Choong et al., 2021; Abu-Shanab et al., 2020) emphasize the

importance of fostering positive security attitudes through effective communication and user-centric policies. Finally, research on practices (Kim et al., 2021) identifies factors influencing behavior and stresses on the need to bridge the gap between knowledge and practice through practical training and positive reinforcement.

In conclusion, the literature review illuminates the intricate relationship between technology, education, and cybersecurity. It highlights the pressing need for educators to be equipped with the skills and knowledge to navigate the cyber space effectively and address emerging cybersecurity challenges. The identified gaps in teacher preparedness, ethical considerations, and institutional cybersecurity vulnerabilities underpin the importance of research initiatives in this aspect. By examining the effectiveness of such interventions, we can contribute to building a more secure and resilient digital learning environment for all.

As published research studies on the effectiveness of any cybersecurity training programme comprehensively focused on the aspects of cybersecurity under consideration were not available, null hypotheses were framed.

Methodology: This study is quantitative in nature based on the positivist approach. This research aimed to evaluate the effectiveness of a cybersecurity training programme for student teachers. Hence, one-group pre-test-post-test was more appropriate considering the constraints. The participants in this study consisted of fifty student teachers enrolled for the B.Ed. programme. The sample represented diverse group of individuals poised to enter the teaching profession. The tool prepared by the researcher consisted of multiple sections aligned with the key aspects of cybersecurity literacy. It was divided into four sections; knowledge, awareness, attitude, and practices. Each section aimed to capture specific aspects of participants' proficiency in understanding the workings of the internet, awareness of virtual dangers, attitude towards cybersecurity, and practices adopted to ensure online safety. The tool was validated with the help of experts' opinions and test-retest reliability was found to be 0.678.

Data Collection: The data collection process involved conducting a pre-test to assess the initial level of cybersecurity awareness among participants. Following the pre-test analysis, a thirty-hour programme on cybersecurity literacy was administered. The sessions were spread over two months. Upon the completion of the programme, a post-test was administered. The results of the Pre-test and Post-test were compared.

Data analysis:

Objective 1 To design a programme on cybersecurity for student teachers.

Design of the training programme: The training programme was designed as a thirty-hour cybersecurity literacy programme with a primary emphasis on four key aspects: knowledge,

awareness, attitude, and practices. The programme adopted a blended mode of delivery, combining online and face-to-face sessions. Each module of the programme included a set of planned activities, such as case studies, practicum, quizzes, and assignments, to enhance learning beyond the classroom. Reading materials were also provided to the students as part of the programme resources.

Objective 2: To study the perceived effectiveness of the training programme on different aspects of cybersecurity literacy, such as knowledge, awareness, attitude, and practices.

Quantitative data analysis methods were employed to assess the effectiveness of the cybersecurity training programme on the variables. Descriptive statistics were used to summarize the Pre and Post-test levels of knowledge, awareness, attitude, and practices. Paired-sample t-test was applied to determine the statistical significance of the difference between the Mean scores of these variables.

Table No. 1.1

	Pre test		Post Test		t value	p value	Null Hypothesis
	Mean	SD	Mean	SD			
Knowledge	20.58	2.81	24.20	2.25	7.890	0.0001	Rejected
Awareness	21.08	2.23	23.94	2.11	7.243	0.0001	Rejected
Attitude	6.54	0.84	7.88	1.12	7.452	0.0001	Rejected
Practices	17.84	3.09	20.64	2.82	6.352	0.0001	Rejected
Aggregate	24.92	2.88	29.30	2.75	8.897	0.0001	Rejected

Interpretation: The paired t-test statistics show that the mean of post-test scores is significantly higher than the mean of the pre-test scores, for all the four aspects (Knowledge, Awareness, Attitude and Practice); and also, for the mean score of the aggregate post-test and pre-test. The p-value is 0.0001 in each case which is less than 0.05, hence the null hypothesis is rejected. This shows that the training programme is effective in enhancing the Knowledge, Awareness, Attitude and Practice of cyber security. Students have shown significant gain in the total score at the post-test level as well.

Objective 3: To study the correlations between different aspects of cybersecurity literacy such as knowledge, awareness, attitude, and practices.

Table No. 1.2

	Knowledge	**Awareness**	**Attitude**	**Practices**
Knowledge	1			
Awareness	.930**	1		
Attitude	.537**	.636**	1	
Practices	.623**	.599**	.536**	1

***. Correlation is significant at the 0.01 level (2-tailed).*

Interpretation: The correlation analysis reveals strong and statistically significant relationships among different aspects of cybersecurity literacy. Table 1.2 shows that all the aspects show positive significant correlation, indicating that both the aspects move in the same direction and the relationship is significant at 0.01 level.

The cybersecurity practices of the student teachers were recorded at the pre and post-test levels. The data was analysed based on the frequencies under each practice.

Table No. 1.3

Behavioural Changes	**Pre-Test**	**Post -Test**
Password Changes	19	23
Licenced Antivirus	5	13
Safe Browsing	26	26
Two factor authentication,	0	10
Personal Information Limited	0	11
None	6	0

Interpretation: The data presented reflects student teachers' self-reported changes in cybersecurity practices before (Pre-Test) and after (Post-Test) the training programme. The results indicate perceived improvements in specific cybersecurity practices.

The change in the behaviour is quite noticeable at the post-test level with reference to password change, secured browsing as regards to not leaving digital information and minimise using free Wi-Fi, using licensed antivirus, two factor authentication, and likewise. This shows that the students have become more cautious about the data security. They have learnt that Prevention is better than Cure!

Discussion: The results highlight significant improvements in student teachers' cybersecurity knowledge, awareness, attitude, and practices post-training, validating the efficacy of the

intervention. The student teachers, being part of the younger generation, might have a basic awareness of cyber safety and take precautions at a fundamental level. However, they might lack knowledge about more severe cyber threats.

The paired-samples statistics reveal substantial enhancements in overall cybersecurity literacy, with a notable increase in mean scores from pre-test to post-test across all aspects. The statistically significant improvements indicate that the training programme effectively augmented student teachers ' understanding of cybersecurity concepts. This emphasizes the programme's success in bridging the initial proficiency gaps and equipping participants with a comprehensive grasp of cybersecurity fundamentals.

The correlation analysis unravels the interconnected nature of cybersecurity literacy aspects among student teachers. The strong positive correlations highlight the symbiotic relationships among knowledge, awareness, attitude, and practices. These findings suggest that as student teachers enhance their knowledge, they are more likely to develop positive attitudes and adopt best practices in cybersecurity. The interplay of these aspects emphasizes the holistic nature of cybersecurity literacy, advocating integrated approaches in training programmes.

The study aligns with the literature highlighting the ethical responsibilities of educators in the digital realm. The observed improvements in student teachers' awareness and practices address ethical considerations, such as cyberbullying prevention and safeguarding data. The training programme appears to have instilled a sense of ethical responsibility among student teachers, aligning with the broader societal expectations for educators in the digital age.

Future Implications and Recommendations: The study advocates the integration of cybersecurity education into formal teacher education programmes. By embedding cybersecurity principles within the broader education curriculum, institutions can proactively prepare educators for the evolving digital environment.

Recognizing the evolving nature of cybersecurity threats, institutions should establish continuous professional development programmes. These programmes should provide regular updates to educators, ensuring they stay abreast of the latest cybersecurity trends, technologies, and best practices to ensure that teachers are well-prepared to adapt to the rapidly changing digital landscape.

Conclusion: The research paper encapsulates a transformative journey—from recognizing the challenges posed by the digital shift in education to implementing, a training programme aimed at stimulating student teachers. The narrative unfolds against the backdrop of the digital era, portraying the evolution of teacher preparedness and the proactive measures taken to address cybersecurity concerns. Ongoing training is identified as a critical component for educators.

As technology continues to advance, educators must remain adaptable and resilient, equipped with the knowledge and skills to safeguard students in the ever-evolving digital space. With the advancement in technology, it is crucial to recognize that new cybersecurity challenges will emerge, emphasizing the need for regularly updating training programmes to address evolving threats.

References:

Bates, T. (2016). Teaching in a Digital Age: Guidelines for designing teaching and learning. Tony Bates Associates.

Crosslin, M., Benham, B., Dellinger, J., Patterson, A., Thomas, R., & Dellinger, J. (2017). Ethical considerations in digital teaching and learning. In Handbook of Research on Humanizing the Distance Learning Experience in the Digital Age (pp. 270-285). IGI Global.

Crosslin, M., Dellinger, J., Joksimović, S., Gasevic, D., & Brooks, C. (2017). Ethics and Privacy in Educational Technology: A Review of Current Practices in Four Leading Journals. Educational Technology Research and Development, 65(5), 1183-1206.

Ertmer, P. A., Ottenbreit-Leftwich, A. T., Sadik, O., Sendurur, E., Sendurur, P., & Yu, F. Y. (2012). Teacher beliefs and technology integration practices: A critical relationship. Computers & Education, 59(2), 423-435.

Graeber, M., Medlin, A. C., & Sasse, M. A. (2019). The role of attitudes in cybersecurity: Towards a model of user security behavior. Computers & Security, 88, 101727.

Johnson, L., Adams Becker, S., Estrada, V., & Freeman, A. (2015). NMC/CoSN Horizon Report: 2015 K-12 Edition. The New Media Consortium.

Koehler, M. J., & Mishra, P. (2009). What is technological pedagogical content knowledge (TPACK)?. Contemporary Issues in Technology and Teacher Education`, 9(1), 60-70.

Mancuso, C. (2020). Cybersecurity in education: A guide for schools and colleges. Routledge.

Mancuso, C. (2020). Cybersecurity Challenges in Educational Institutions: A Case Study Analysis. Journal of Information Systems Education, 31(3), 107-119.

Rezai, M. J., & Salehahmadi, Z. (2019). Information security awareness: An educational paradigm. Journal of Information Security and Applications, 44, 109-118.

Rezai, M. J., & Salehahmadi, Z. (2019). Cybersecurity education for K-12 teachers: A content analysis of teacher guides. Computers & Education, 142, 103642.

Selwyn, N. (2017). Education and Technology: Key Issues and Debates. Bloomsbury Publishing.