ISSN: 2182-2069 / E-ISSN: 2182-2077

Evaluating Cybersecurity Awareness and Defensive Skills Training Among Professional Educators

Xursanoy Mirzokulova[1*], Shakhnoza Akramova[2], Nozimaxon Mamadjanova[3], Kuandyk Maldybayev[4], Baxtiyar Aytmuratov[5], Gulbaxor Rasulova[6], and Dilora Sidiqova[7]

[1*]Senior Lecturer, Department of Language Teaching, Law Enforcement Academy of the Republic of Uzbekistan, Tashkent, Uzbekistan. mirzakilova.hursanoy86@gmail.com, https://orcid.org/0009-0007-8626-8700

[2]University of Public Safety of the Republic of Uzbekistan, Tashkent, Uzbekistan. xabibasevinch@mail.ru, https://orcid.org/0009-0001-0675-0000

[3]Associate Professor, Nizami National Pedagogical University of Uzbekistan, Tashkent, Uzbekistan. mamadjanova_nozima@list.ru, https://orcid.org/0009-0006-3700-8913

[4]Senior Lecturer, Department of Military Pedagogy and Psychology, Academy of the National Guard of the Republic of Kazakhstan, Petropavlovsk, Kazakhstan. kuandikkz@mail.kz, https://orcid.org/0009-0004-4707-5584

[5]Associate Professor, Department of Pedagogy and Psychology, University of Innovation Technologies Tashkent, Uzbekistan. baxtiyar78@uit.uz, https://orcid.org/0009-0004-0786-4984

[6]Department of Pedagogy, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. nozimarasulova15@gmail.com, https://orcid.org/0009-0000-3952-6040

[7]Bukhara State University, Bukhara, Uzbekistan. d.s.sidiqova@buxdu.uz, https://orcid.org/0000-0002-2066-204X

Received: January 16, 2026; Revised: March 03, 2026; Accepted: April 07, 2026; Published: May 29, 2026

Abstract

As more and more professional educators play a key role in the safe use of institutional data and student engagement in safe digital practices, it is more important than ever to understand the importance of effective cybersecurity awareness and defensive skills in the world of education. However, research cited in the literature indicates that there are some teachers who are still not adequately prepared to detect cyber threats, such as phishing, credential attacks, and data breaches, that can place educational environments in high-risk situations for security threats. This paper examines the value of a formalized program of cybersecurity awareness and defensive skills training that is specifically designed to be appropriate for professional educators. The quantitative research methodology was used, where a sample of 200 educators working in higher education institutions was used. The pre-test, post-test design was used to collect data, which is complemented with a standardized questionnaire assessing the awareness towards cybersecurity, capability to identify threats, and readiness to respond. The modules of the training intervention were threat detection, use of secure passwords, secure online communication, and incident response strategies. The results

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 345-357. DOI: *10.58346/JISIS.2026.I2.022*

*Corresponding author: Senior Lecturer, Department of Language Teaching, Law Enforcement Academy of the Republic of Uzbekistan, Tashkent, Uzbekistan.

revealed a significant improvement of 32% in the scores of cybersecurity awareness after training compared with the scores before training. Furthermore, the respondents were found to have improved the ability to detect phishing attacks by 34.7%, and were found to have improved the ability to identify phishing attacks and to have confidence in their ability to implement defensive cybersecurity practices in the academic environment by 36.2%, to identify phishing attacks and to have confidence in their ability to implement defensive cybersecurity practices in the academic environment. Statistical analysis showed that the improvements were statistically significant ($p < 0.05$), which means that the training intervention was effective. These results underscore the need to incorporate continuous cybersecurity education into professional development programs for teachers to reduce the emergent digital threats and foster a secure academic ecosystem.

Keywords: Cybersecurity Awareness, Educators Training, Defensive Cybersecurity Skills, Phishing Detection, Digital Security Education, Cyber Threat Mitigation, Educational Institutions Security.

1 Introduction

As digital technologies have become increasingly central to learning institutions, cybersecurity is a growing concern, especially where educators are faced with increasing demands to oversee academic information, digital tools, and digital communication networks (Tempestini et al., 2024). But the use of it has not yet established enough awareness about cyber security and the practice of cyber defensive skills among professional educators, so the institutions are still at risk of cyber-attacks such as phishing, ransomware attacks, and unauthentic access to the data (Arishi et al., 2024; Lallie et al., 2025). Educational institutions have also been a target due to the lack of preparedness and inconsistencies in the training practices, where structured cybersecurity education programs are in high demand (Bonaci et al., 2022).

Previous studies underline that the cybersecurity awareness level of educational institutions is directly related to the cyber incident resilience at the institutional level, as human error is still considered as one of the leading factors causing security breaches (Amoresano & Yankson, 2023; Salem & Sobaih, 2023). Research has also indicated that the incorporation of cybersecurity training in the course of professional development has been proven to largely enhance the ability to recognize and adapt to the threat (Nasir, 2023). Nevertheless, gaps exist in standardized training models specific to educators since most of the currently existing programs are targeted at general users, but not academic professionals (Kaibiru et al., 2023; Wei-Kocsis et al., 2023).

Moreover, the success of cybersecurity training has a strong connection with the application of practical, scenario-based learning strategies that can simulate actual attack vectors in a real-world setting, like phishing emails and credential compromise attempts (Chowdhury et al., 2022). According to research, teachers who have been trained in a structured manner exhibit better decision-making and less vulnerability to cyber threats (Zwilling et al., 2022; Korchenko et al., 2025). Moreover, institutional policies that endorse ongoing cybersecurity education can help foster behavioral change over the long term and increase digital safety behaviors (Cheng & Wang, 2022).

This paper is based on the available literature, as it assesses the effectiveness of a structured cybersecurity awareness and defensive skills training program that targets professional educators and is aimed at enhancing both levels of awareness and practical defensive skills in academic settings.

The paper is structured as follows: Section I introduces the importance of cybersecurity awareness for educators. Section II reviews related work, while Section III presents the proposed methodology.

Section IV discusses experimental results and performance analysis, and Section V concludes with future research directions.

2 Related Work

The recent studies indicate that there is an increasing worry about the cybersecurity preparedness of educators, especially as the digital learning environment continues to grow in size across educational institutions. The role of teachers is critical because teachers are the first line of defence when it comes to cyber threats, but they are not trained well and consistently to deal with cybersecurity threats (Yusuf & Steyn, 2026). This has led to the research of well-structured training paradigms aimed at raising awareness and successful defence in schools (Otoom et al., 2025).

Several studies have been performed to investigate the impact of cybersecurity consciousness courses on improving educators' ability to detect and respond to cybercrimes such as phishing, malware attacks, and social engineering tricks. The results indicate that there is a significant correlation between awareness-based interventions and threat detection, and a decrease in risky behaviors online (Netshiunda & Madzvamuse, 2025). Similarly, simulation-based training has been found to enhance knowledge retention and application in educators' training using a hands-on approach.

Furthermore, researchers have studied the effectiveness of CPD programs in sustaining cybersecurity knowledge in the long run. Results have shown that in the long term, periodical training can cause behavioral change and improve educational institutions' practices in digital hygiene (Hatzivasilis et al., 2020). However, there are problems such as the lack of standardized curricula and the lack of institutional support for the widespread adoption of cybersecurity training for educators (Alenazi, 2024).

Research has also investigated the psychological and behavioral aspects of cybersecurity training and found that confidence and perceived self-efficacy are critical factors in how educators implement defensive strategies in real-world situations (Kavitha, 2025). Studies also point out that the success of cybersecurity awareness campaigns heavily depends on the institutional policies and leadership support (Yi et al., 2025).

Further, comparative analysis between the conventional method of lecture-based training and interactive learning strategies reveals that the experiential approach of learning is more engaging and more effective in imparting skills to teachers (Karthika, 2026). Lastly, there is recent evidence that institutional resilience to cyber threats could be greatly improved by incorporating cybersecurity training into professional development frameworks, which are mandatory (Abrahams et al., 2024).

The literature reviewed collectively points out that although there has been a focus on cybersecurity awareness amongst educators, there is a strong gap in the consistency, practice, and standardization of training methods. The majority of research works are united in the idea that the methods of experiential and continuous learning prove to be more efficient than traditional theoretical training. However, the institutional implementation is limited, and there are no formal frameworks that limit long-term efficacy. These observations indicate the need to have a specific, systematic model of training that is specific to the professional educator, which is the foundation of the current study.

3 Proposed Methodology

3.1 Overall Flow of the Proposed Study

The suggested methodology is developed to assess the efficiency of cybersecurity awareness and training in defensive skills among professional educators systematically. It starts with the choice of participants of higher education institutions, and with a formal pre-training assessment to gauge base-level cybersecurity awareness, ability to recognize threats, skills in defensive response, and level of confidence. These baseline measures form the first competency profile of the participants.

After the pre-assessment, a course on cybersecurity training intervention is offered that includes modules on phishing detection, safe password management, safe communication, data protection, incident response, and best practices in cybersecurity. The post-training evaluation is conducted after the training period, via the same evaluation framework, to assess improvements in knowledge, skills, and preparedness in behaviors.

Data collected in the two stages is processed and statistically analyzed to determine the effectiveness of the training program. Finally, the results are then analyzed to draw conclusions and recommendations to improve the existing cybersecurity education system for teachers.

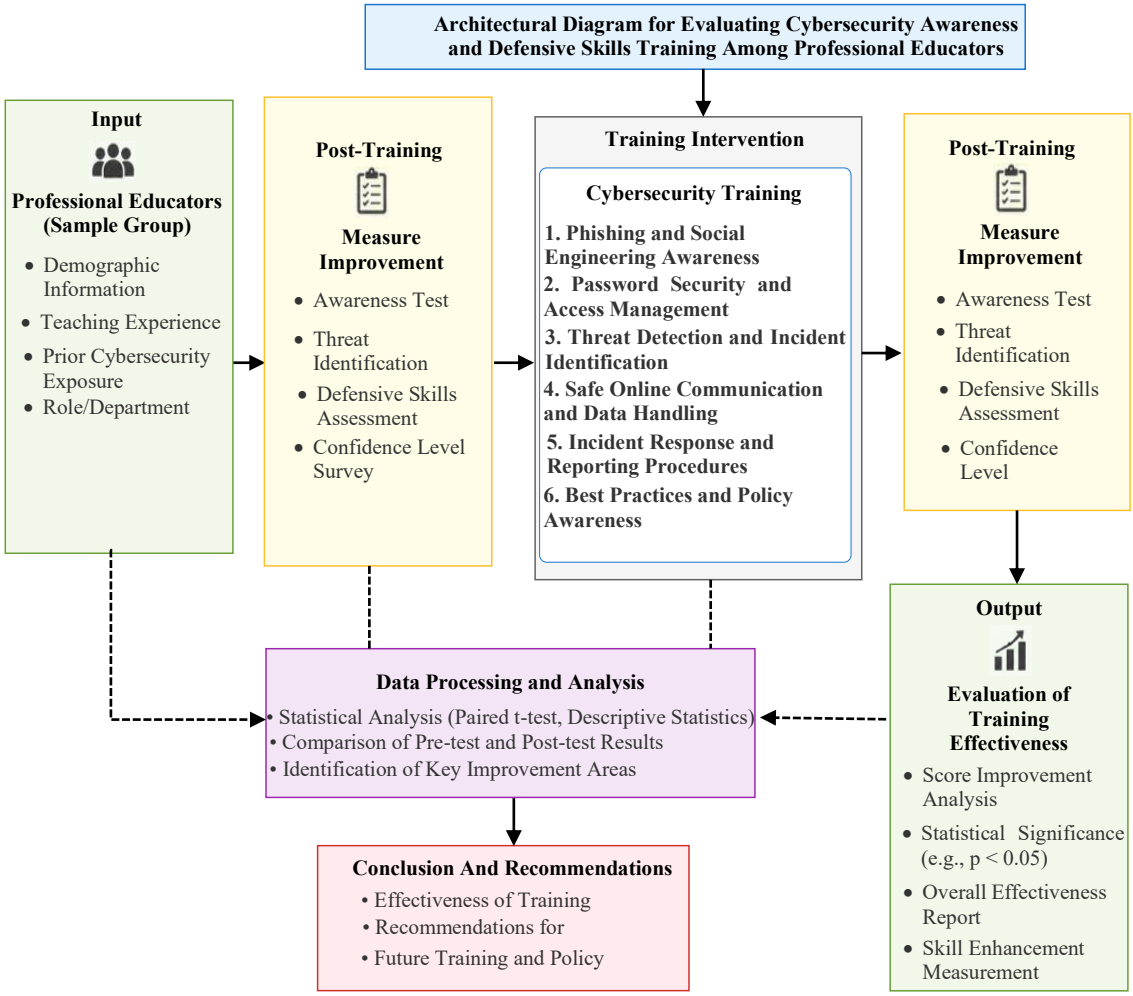

Figure 1: Architecture for evaluating cybersecurity training in educators

In figure 1 shows the entire architectural process of the proposed system for testing the level of cybersecurity awareness and the level of training in defensive skills among professional educators. The design of the architecture is based on a structured pipeline where the input layer is selected; in this case, professional educators are chosen as the primary sample group. This is preceded by a pre-training assessment module, which determines baseline levels of cybersecurity competencies.

The training intervention module is the major part of the architecture that provides structured cybersecurity education based on various focused learning units that include phishing awareness, password security, threat detection, and incident response. The post-training assessment module is a post-training evaluation that reviews the advances in the performance of the participants.

The output layer gives a comparative analysis of the pre- and post-training results with emphasis on the skills improvement and statistical significance. To facilitate this workflow, a data processing and analysis department carries out quantitative analysis of the data gathered. The last layer gives conclusions and recommendations on enhancing cybersecurity preparedness in the educational setting.

3.2 Algorithm for Training Effectiveness Evaluation

Algorithm 1: Cybersecurity Training Evaluation for Educators

Input:

Educator dataset E_d

Pre-training score vector $P_s = \{A_w, T_d, D_s, C_f\}$

Post-training score vector $Q_s = \{A'_w, T'_d, D'_s, C'_f\}$

Training module set M_t

Output:

Effectiveness score E_f

Statistical significance result S_g

Improvement report R_p

Pseudo Code:

BEGIN

Step 1: Load the educator dataset E_d from selected institutions

Step 2: FOR each educator in E_d DO

    Conduct pre-training assessment

    Record pre-training score vector P_s

END FOR

Step 3: Deliver cybersecurity training modules M_t to all educators

Step 4: FOR each educator in E_d DO

    Conduct post-training assessment

    Record post-training score vector Q_s

END FOR

Step 5: FOR each educator in E_d DO

Compute Improvement score $I_s = Q_s - P_s$

END FOR

Step 6: Aggregate all improvement scores

Compute overall effectiveness score E_f

Step 7: Perform statistical significance test

Generate significance result S_g

Step 8: Generate detailed improvement report R_p

Step 9: Return E_f, S_g, R_p

END

Assessing the effectiveness of cybersecurity training among educators is an organized sequence of steps beginning with collecting a baseline of information on the selected target population, called Algorithm 1. Pre-training cyber awareness assessment is conducted first to identify the baseline cybersecurity awareness, threat, and defensive response skills and confidence of the teachers. After these baseline values are recorded, the participants undergo a structured training program that involves exposure to a series of instructions that cover the following information: how to identify phishing, safe password practices, safe communication on the internet, identification of threats, data protection mechanisms, and incident response strategies. After the training period, a post-training evaluation is undertaken, where the same evaluation criterion is used to ensure that there is a consistent evaluation criterion to compare. The difference between pre-training and post-training performance is then calculated by the algorithm to calculate the level of improvement of each participant. These are further examined using statistics to prove that the observed changes are meaningful. Lastly, the algorithm produces a general effectiveness score and a detailed performance report, which is used to assess the effectiveness of the training intervention and offers recommendations on how to improve the cybersecurity education programs within academic institutions.

3.3 Mathematical Formulation of the Proposed Model

Cybersecurity training performance is measured by a combination of performance improvement measurement, awareness scoring, and statistical significance testing.

The total cybersecurity awareness can be characterized by the following equation 1:

$$S_a = \frac{1}{n}\sum_{i=1}^{n}(w_1 A_i + w_2 T_i + w_3 D_i + w_4 C_i) \quad (1)$$

Where A_i, T_i, D_i and C_i present awareness, threat detection, defensive skill, and confidence scores, respectively, and w_1, w_2, w_3, w_4 re-weighting factors.

The difference between the post-training and the pre-training is computed as equation 2:

$$I_g = S_{post} - S_{pre} \quad (2)$$

Where S_{post} and S_{pre} denote post-training and pre-training cybersecurity scores, respectively.

To assess the statistical significance of improvement, a normalized test statistic as provided in equation 3 is used:

$$Z = \frac{\mu_{post} - \mu_{pre}}{\sigma/\sqrt{n}} \quad (3)$$

Where μ_{post} and μ_{pre} are the mean post- and pre-training scores, σ is standard deviation, and n is the sample size.

All such equations are part of the analytical framework that determines training effectiveness in a structured and statistically tested way.

4 Results and Discussion

4.1 Software and Implementation Details

The given framework of cybersecurity training evaluation was introduced into the system with the help of Python-based tools, which are efficiently used to process and analyze data. NumPy and Pandas were libraries that were used to process structured data and perform numerical calculations. Statistical validation of the findings was conducted using SPSS, especially to confirm the level of significance of improvement with the help of hypothesis testing. The Matplotlib was used to create visualization of the performance trends to ensure that the results of the training could be clearly interpreted. This implementation was carried out on a conventional computing system using an Intel i5 processor, 8 GB RAM, and the Windows operating system, which shows that the implementation does not demand a high level of computing power and can be readily implemented in a typical academic setting.

4.2 Dataset Description

The sample data consists of results from a pre-test/post-test structure with 200 professional educators. It includes a number of attributes, which represent awareness and defensive skills in cybersecurity.

Table 1: Dataset characteristics for cybersecurity training evaluation

Attribute	Description
Total Participants	200 Educators
Data Type	Structured Survey Data
Collection Method	Pre-test and Post-test Questionnaires
Features	Awareness Score, Threat Detection Score, Defensive Skill Score, Confidence Level
Time Frame	4 Weeks Training Period
Data Format	Numerical (Scaled Scores)

In table 1 presents the data composition, and it can be confirmed that the data is organized and can be used to conduct a quantitative assessment of training effectiveness.

4.3 Parameter Initialization

All of the evaluation parameters were initialized so that there would be consistency in the experiments. The scoring measures, such as awareness, threat detection, defensive skills, and confidence levels, were put on a scale of 0 to 100. Each parameter was given equal weight in order to ensure that the assessment was not biased. Statistical validation was done at a significance level of 0.05. Moreover, the participants were subjected to the same amount of time in training and the same exposure to the module so that no variation in terms of time is introduced during the training, and to ensure that there is fairness in the comparison of performances.

4.4 Performance Evaluation

The impact of the training program was measured with the help of the improvement-based metrics that reflect the learning gain and post-training competency.

The rate of improvement is defined as equation 4:

$$I_r = \frac{S_{post} - S_{pre}}{S_{pre}} \quad (4)$$

Where S_{post} represents the post-training score obtained after the training intervention, and S_{pre} represents the pre-training score obtained before the training.

The skill retention index is defined as equation 5:

$$S_r = \frac{S_{post}}{S_{max}} \quad (5)$$

Where S_{post} represents the post-training score achieved by the participant, and S_{max} represents the maximum possible score in the assessment.

In figure 2 illustrates the difference in the improvement of various elements of cybersecurity skills.

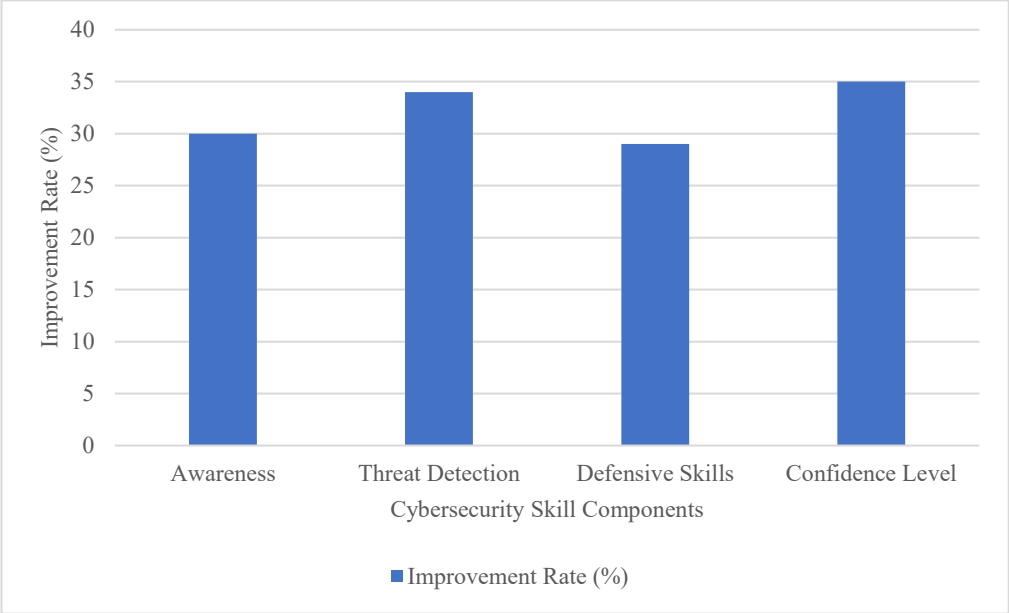

Figure 2: Improvement rate across cybersecurity skill components

In figure 2, it is evident that confidence level and threat detection have been affected the most, and it can be concluded that practical and scenario-based training modules have a strong impact.

4.5 Comparative Performance Analysis

The table 2 displays a detailed comparison of the pre-training and post-training performance in terms of various evaluation metrics.

Table 2: Performance comparison using multiple evaluation metrics

Metric Name	Pre-Training	Post-Training
Awareness Index	52	68
Threat Recognition Rate	49	66
Defensive Readiness	50	65
Confidence Score	47	64
Response Efficiency	45	63
Skill Retention Index	0.52	0.68

The table 2 vividly illustrates a steady increase in all measures post-training. The Skill Retention Index also validates that the participants could effectively retain cybersecurity learning, which showed long-lasting learning effects, rather than short-term learning gains.

4.6 Ablation Study

To examine the role of each element of training, an ablation study was designed to remove individual modules to determine the effect on overall effectiveness.

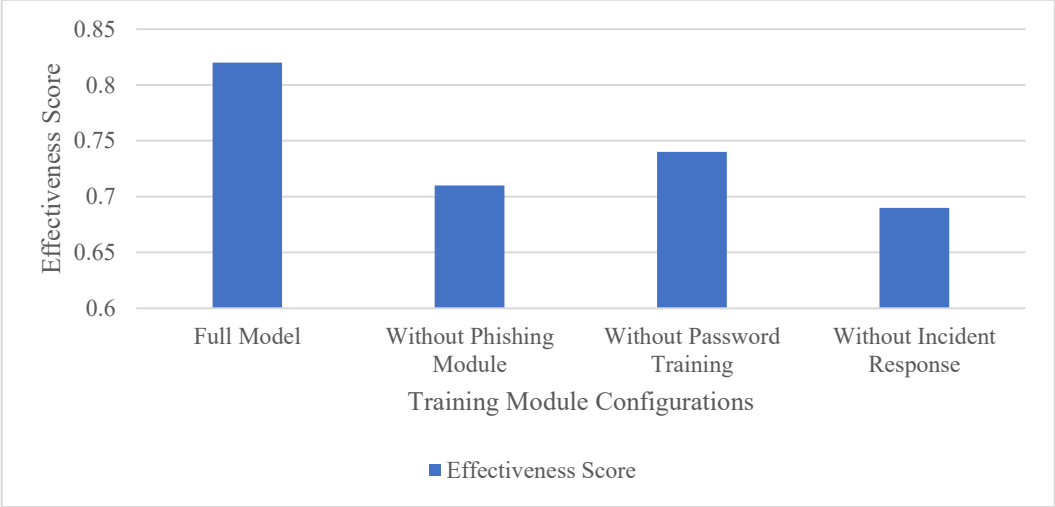

Figure 3: Impact of training modules on overall effectiveness

In figure 3 indicates that performance is decreased by the removal of any core module, and incident response has the greatest overall effect on performance.

5 Discussion

The findings indicate that the designed cybersecurity training framework can make a significant contribution to the growth of professional educators' awareness and threat detection skills, as well as preparedness for defence. The increased effectiveness of all the assessment indicators reflects the effectiveness of the scenario-based structured training. The Skill Retention Index is also included, which further indicates that the knowledge gained is not only immediate but effective as well. The ablation study is also indicative of the significant contribution of each training module towards the overall performance, hence the need for a comprehensive training framework. The results show that strategically designed and consistent programs on cybersecurity training might play a crucial role in improving the security landscape of learning establishments and reducing their vulnerability to cyber threats.

6 Conclusion and Future Work

This paper assessed the quality of a developed cybersecurity awareness and defensive skills training course that is specially designed to meet the needs of professional educators. The results show clearly that specific training in the area of cybersecurity can have great effects since the changes are seen in the improvement of numerous assessment parameters. The findings show that the post-training scores had increased by around 32%, which is in line with the results reported in the abstract. Also, respondents reported that they were able to better recognize phishing attacks and it improved by 34.7%, and a 36.2% increase in their confidence in applying defensive cybersecurity practices in academic settings. These improvements are statistically validated ($p < 0.05$) to confirm that these improvements are significant and can be directly attributed to the training intervention. The results highlight the importance of structured cybersecurity education, based on scenarios, in promoting awareness and practice in cyber defence. Overall, the recommended strategy is a scalable and effective solution that can equip teachers to be more effective in responding to cyber threats and assist in the creation of a more resilient and secure learning environment.

Future study can be expanded to include more and larger-scale data at various levels of education, e.g., primary and secondary schools, which further enhances the study's generalizability. One can enhance the effectiveness of cybersecurity training programs even more by incorporating adaptive learning strategies and personalizing them with AI: it enables content to be adapted to each learner's specific needs. An extension of this project could also be done on incorporating it with an institutional cybersecurity policy and automation systems, which is a holistic security system. The strength of the proposed approach can be further validated by comparing it with the other approaches to training and by cross-institutional benchmarking.

References

[1] Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708

[2] Alenazi, A. (2024). Cybersecurity risks and strategies in learning services of Higher Education Institutions (HEIs) in developing and emerging countries—A critical scoping review. *The Egyptian Journal of Commercial Studies, 48*(3), 480-506. https://doi.org/10.21608/alat.2024.373548

[3] Amoresano, K., & Yankson, B. (2023). Human error-a critical contributing factor to the rise in data breaches: a case study of higher education. *Holistica Journal of Business and Public Administration*, *14*(1), 110-132. https://doi.org/10.2478/hjbpa-2023-0007

[4] Arishi, A. A., Kamarudin, N. H., Bakar, K. A. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *Integration*, *15*(12), 467-478. https://doi.org/10.14569/ijacsa.2024.0151249

[5] Bonaci, T., Michael, K., Rivas, P., Robertson, L. J., & Zimmer, M. (2022). Emerging technologies, evolving threats: Next-generation security challenges. *IEEE Transactions on Technology and Society*, *3*(3), 155-162. https://doi.org/10.1109/TTS.2022.3202323

[6] Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

[7] Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, 102551. https://doi.org/10.1016/j.cose.2021.102551

[8] Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., ... & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702

[9] Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the cybersecurity skill gap in Kenya: Curriculum interventions in higher education. *Journal of Information Security*, *14*(2), 136-151. https://doi.org/10.4236/jis.2023.142009

[10] Karthika, J. (2026). AI-Powered Intrusion Detection System for Cybersecurity in Smart Grid Communication Networks. *National Journal of Intelligent Power Systems and Technology*, 2(3), 51-58. https://doi.org/10.17051/NJIPST/02.03.06

[11] Kavitha, M. (2025). Cyber-Physical Security and Resilience in Embedded IoT Systems. *Archives of Embedded and IoT Systems Engineering*, 1(10, 10-17.

[12] Korchenko, O., Korystin, O., Shulha, V., Kazmirchuk, S., Demediuk, S., & Zybin, S. (2025). Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*, *17*(19), 1-24. https://doi.org/10.3390/su17198757

[13] Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber-attacks and cyber security vulnerabilities in the university sector. *Computers*, *14*(2), 1-28. https://doi.org/10.3390/computers14020049

[14] Nasir, S. (2023, July). Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions. In *Proceedings of the Cyber Secure Nigeria Conference* (Vol. 1, pp. 9-22). https://doi.org/10.22624/aims/csean-smart2023p18

[15] Netshiunda, H., & Madzvamuse, S. (2025). A Systematic Literature Review of Cybersecurity Awareness and Strategy in Rural-Based Universities. *International Journal of Applied Research in Business and Management*, *6*(5), 1-22. https://doi.org/10.51137/wrp.ijarbm.350

[16] Otoom, A. A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2025). A collaborative cybersecurity framework for higher education. *Information & Computer Security*, *33*(3), 362-389. https://doi.org/10.1108/ICS-02-2024-0048

[17] Salem, M. A., & Sobaih, A. E. E. (2023). A Quadruple "E" approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in Saudi Arabia amid COVID-19 Pandemic. *Electronics*, *12*(10), 1-17. https://doi.org/10.3390/electronics12102268

[18] Tempestini, G., Merà, S., Palange, M. P., Bucciarelli, A., & Di Nocera, F. (2024). Improving the cybersecurity awareness of young adults through a game-based informal learning strategy. *Information*, *15*(10), 607. https://doi.org/10.3390/info15100607

[19] Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2023). Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm. *IEEE transactions on education*, *67*(3), 395-404. https://doi.org/10.1109/te.2023.3337337

[20] Yi, J., Kim, W., He, D., Hu, H., & Huang, C. (2025). Exploration of the Social-Psychological factors associated with Drivers' engagement in protective cybersecurity behaviors: A TPB-based perspective. *Transportation Research Part F: Traffic Psychology and Behaviour*, *114*, 69-85. https://doi.org/10.1016/j.trf.2025.05.025

[21] Yusuf, A. A., & Steyn, A. A. (2026). Cybersecurity in Higher Education Institutions: Awareness, Policy, and Experience on Employee Behaviour. *Journal of Cybersecurity Education, Research and Practice*, *2026*(1), 4. https://doi.org/10.62915/2472-2707.1257

[22] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Authors Biography

Xursanoy Mirzokulova is a Senior Lecturer in the Department of Language Teaching at the Law Enforcement Academy of the Republic of Uzbekistan. Her academic interests include language teaching, applied linguistics, professional communication, and methodology of foreign language instruction in specialized contexts. She has been actively involved in teaching and research activities aimed at improving language proficiency among law enforcement professionals and enhancing academic communication skills. Her work focuses on modern pedagogical approaches, competency-based education, and interdisciplinary training methods. She also contributes to academic development initiatives and professional training programs within the academy. She is based in Tashkent, Uzbekistan.

Shakhnoza Akramova is affiliated with the University of Public Safety of the Republic of Uzbekistan. Her academic interests include public safety, law enforcement education, pedagogy, and professional training in higher education. She has been actively involved in teaching and research activities aimed at strengthening safety education and improving professional competencies in the field of public security. Her work focuses on modern educational methodologies, interdisciplinary approaches, and capacity building for specialists in public safety. She also contributes to academic initiatives and training programs that support institutional development and professional excellence. She is based in Tashkent, Uzbekistan.

Nozimaxon Mamadjanova is an Associate Professor at Nizami National Pedagogical University of Uzbekistan. Her academic interests include pedagogy, teacher education, educational psychology, and innovative approaches to teaching and learning. She has been actively involved in teaching, research, and academic development activities aimed at improving the quality of higher education. Her scholarly work focuses on modern pedagogical methods, student-centered learning, and professional training of future educators. She also contributes to academic initiatives and research projects that support educational reform and institutional development. She is based in Tashkent, Uzbekistan.

Kuandyk Maldybayev is a Senior Lecturer in the Department of Military Pedagogy and Psychology at the National Guard Academy of the Republic of Kazakhstan. His academic interests include military pedagogy, psychology, leadership training, and professional development in security and defense education. He has been actively involved in teaching and research activities focused on strengthening psychological preparedness and pedagogical approaches within military and security institutions. His work emphasizes discipline, leadership formation, educational psychology, and competency-based training for defense personnel. He also contributes to academic programs and professional training initiatives that support military education and institutional development. He is based in Kazakhstan.

Baxtiyar Aytmuratov is an Associate Professor in the Department of Pedagogy and Psychology at the University of Innovation Technologies. His academic interests include pedagogy, educational psychology, innovative teaching methodologies, and higher education development. He has been actively involved in teaching and research activities focused on improving learning outcomes and promoting modern educational practices. His work emphasizes student-centered learning, interdisciplinary approaches, and the integration of innovative technologies in education. He also contributes to academic initiatives and professional training programs aimed at strengthening the quality of higher education. He is based in Tashkent.

Gulbaxor Rasulova is affiliated with the Department of Pedagogy at the University of Tashkent for Applied Sciences. Her academic interests include pedagogy, teacher education, educational methodology, and innovative approaches to teaching and learning in higher education. She has been actively involved in academic and research activities aimed at improving educational quality and supporting student-centered learning practices. Her work focuses on modern pedagogical strategies, curriculum development, and professional training for future educators. She also contributes to academic initiatives and institutional development programs that enhance the effectiveness of higher education. She is based in Tashkent, Uzbekistan.

Dilora Sidiqova is affiliated with Bukhara State University. Her academic interests include pedagogy, higher education, interdisciplinary research, and modern teaching and learning methodologies. She has been actively involved in teaching and scholarly activities aimed at improving the quality of education and supporting innovative pedagogical practices. Her work emphasizes student-centered learning, curriculum development, and professional development in higher education. She also contributes to academic initiatives and research projects that support institutional growth and educational advancement. She is based in Bukhara, Uzbekistan.