International Research Journal of MMC (IRJMMC)
ISSN 2717-4999 (Online) | 2717-4980 (Print)
Volume 6, Issue 3 │ August 2025 │Special Issue

Evaluating the Behavioural Impact of Machine Learning-Driven Cybersecurity Awareness Programs in Telecommunication Networks

Basanta Lingthep

Corresponding Author
Basanta Lingthep
Email: blingthep@gmail.com

To Cite this article: Lingthep, B. (2025). Evaluating the Behavioural Impact of Machine Learning-Driven Cybersecurity Awareness Programs in Telecommunication Networks. International Research Journal of MMC, 6(3), 66–77. https://doi.org/10.3126/irjmmc.v6i3.83012

Submitted: 17 April 2025 **Accepted:** 6 May 2025 **Published:** 7 August 2025

Abstract

The increasing frequency and sophistication of cyberattacks on telecommunication networks require sophisticated techniques for raising the awareness of users and encouraging secure online conduct. This study explores the behavioural effects of machine learning-based cybersecurity awareness programs deployed on telecommunication and computer systems. The main objective is to assess the impact of these data-informed programs on participants' awareness of cyber threats and encourage the uptake of secure behaviours, such as the use of strong passwords, detection of phishing attacks, and secure management of personal information. A mixed-methods design was used, combining pre- and post-program surveys, statistical analysis using SPSS (paired t-tests, chi-square), and transformer-based analysis with Explainable AI (XAI). The research included 500 participants across five telecommunication networks, chosen using stratified random sampling to provide representative findings in technical and non-technical areas. Statistically significant increases in cybersecurity knowledge ($t = 8.76$, $p < 0.001$) and behaviour were found, with significant increases in high-awareness scores (from 25% to 60%) and in important actions like turning on multi-factor authentication and not clicking on phishing links. BERT-XAI analysis indicated a 63% increase in open-ended mentions of proactive security practices, providing interpretable, individualized behavioural insights. The results show the promise of machine learning-based awareness programs to deliver adaptive and quantifiable effects on user behaviour. The findings affirm the embedding of smart education models within telecommunication infrastructures and offer real-world advice for scalable, data-driven cyber education strategy design that continues to prove effective and valid in the face of changing digital threats.

Keywords: cybersecurity awareness, machine learning, behavioural impact, telecommunication networks, cyber hygiene

1. Introduction

The ever-growing complexity of telecommunications networks and the changing reality of cyber threats have made it all the more essential for effective cybersecurity strategies[1], [2]. User awareness generation is one of the main pillars of successful cybersecurity because, historically, human behaviour has been one of the most crucial factors in reducing or enhancing the risks of cybercrime [3], [4]. Traditional approaches to measuring the effectiveness of cybersecurity awareness programs have been constrained by the fact that they are dependent on manual surveys or preset behavioural markers that are simply arbitrary as well as potentially biased[5]. A new strategy for assessing the behavioural impact of such programs becomes available with the advent of machine learning (ML), and we have the greatest example in hand with the advent of the models like BERT [6]. By drawing off BERT's deep contextual knowledge, cybersecurity researchers can now identify fine behaviour indicators in user response elicitation, allowing for more precise and scalable assessment of awareness programs. Adding explainable (XAI) to this process makes the process even more useful because one can be transparent about decision-making, therefore providing cybersecurity trainers and professionals a sense of what factors are influencing their changes of behaviour. This is important, and particularly in such sensitive fields as cybersecurity, where interpretability is what is key to winning the trust of end users and stakeholders. The behaviour impact evaluation approach based on the Transformer model with BERT + XAI framework offers a new method of measuring not only how well users understand and use awareness content but also how these interventions have influenced future behaviours in telecommunication networks. This methodology throws a significant change by connecting both behavioural and textual data into one.

1.1 Background

Telecommunication networks are becoming more intricate, fluid, and divested in the modern world of 5G and more that feeds increased cybersecurity risks. The combination of mobile communication, cloud computing, IoT and technologies such as edge have enlarged the threat surface hence rendering the static rule-based cybersecurity mechanisms inadequate. The theoretical foundations of this research are embedded in the intersection of Artificial Intelligence (AI), behavioural analytics and explainable systems to strengthen cybersecurity awareness and can react faster. Cybersecurity awareness is not just technical competence which determines the individual behaviour that leads to response to the changing threats. The utilization of transformer models (e.g. BERT, Bidirectional Encoder Representations from Transformers) allows for a more nuanced interpretation of user interaction patterns, command line behaviours, and decision-making routine, when under simulated access under threat scenarios. In addition, Explainable AI (XAI) brings transparency and interpretability to the black-box nature of deep learning models – mandatory for trust and adoption by real world applications. By combining BERT with XAI, this research speculates that AI systems can not only identify and forecast user errors or dangerous conduct but also provide an explanation for such decisions in a form that is easily understandable for man. This theoretical underpinning augments a behavioural evaluation framework that facilitates learning by users via feedback and encourages designers of systems to tune educational strategies for secure network practices.

1.2 Literature Review

Yang and Shami [7] suggested an AutoML-based autonomous Intrusion Detection System (IDS), for improved cybersecurity relating to mobile networks as the industry moves from 5G to 6G. Understanding the increasing complexity of Zero-Touch Networks (ZTNs) and the related cyber risks, the authors created a fully automated framework that removes the existing need for manual intervention in cases of conventional machine learning based IDSs. Their approach makes use of Automated Machine Learning (AutoML) to save them in the general data analytics pipeline, which consists of data preprocessing, feature engineering, model selection, hyperparameter tuning and ensemble learning. Some of the key innovations in the framework include the use of a Tabular Variational Auto-Encoder (TVAE) for automatic data balancing, tree-based algorithms for feature selection, base modelling, and Bayesian Optimization (BO) for hyperparameter optimization, the novel Optimized Confidence based Stacking Ensemble (OCSE) for the integration of models is introduced. The framework was verified using two established datasets and being bigger and better than several other state-of-the-art IDS techniques, the framework performed better through the ability to detect accurately as well as adaptiveness. Their work is a major step toward autonomous cybersecurity in next-generation networks and provides valuable points for facilitating implementation of ML-driven security in telecommunication infrastructures.

Rahmati [8] responded to the increasing issues of securing edge networks with an Explainable and Lightweight Artificial Intelligence (ELAI) framework for cyber threat detection in real-time. With the constraints of the edge environments such as the limited computational resource and distributed architecture, the research criticizes the deficiencies of the traditional deep learning models, especially for their lack of interpretability and expense in computation. In order to overcome such barriers, Rahmati suggested a mixed system that adds interpretable machine learning algorithms to light-weighted deep leaning approaches. The ELAI framework uses the decision trees for the clear rule-based classification, attention based neural networks for fine pattern identification and federated learning for distributed privacy preserving model upgradation from end devices. The framework was tested on rule-based benchmark datasets such as CICIDS and UNSW-NB15 and performed well through various cyberattacks. Results emphasized high detection accuracies, low false positives and considerable reduction in computational overhead vis-à-vis conventional approaches in deep learning. The explainability is a significant contribution of this work which has practical value for security analysts seeking to understand model predictions. In general, this research adds a scalable and efficient AI-based cybersecurity model that is especially appropriate for real-time applications in edge-based telecommunications networks.

Akter et al [9] investigated the critical role of cybersecurity awareness capabilities in mitigating the risk of data breaches within the rapidly expanding digital economy. With the exponential growth of big data and digital transformation initiatives, the study highlights how inadequate awareness can leave organizations vulnerable to evolving cyber threats. Using the dynamic capabilities framework, the research identifies and categorizes key enablers of cybersecurity resilience into three thematic dimensions: personnel capabilities (including knowledge, attitude, and learning), management capabilities (comprising training programs, organizational culture, and strategic orientation), and infrastructure capabilities (such as technological infrastructure and data governance policies). The study emphasizes that enhancing these interconnected dimensions is vital to developing robust cybersecurity awareness and readiness across all levels of an organization. By systematically mapping these capabilities, the work provides a strategic framework for businesses to assess and enhance their cybersecurity awareness posture. This research contributes to the growing body of literature that views human and organizational factors as essential complements to technical cybersecurity solutions, particularly in the context of telecommunication and digital infrastructure sectors.

Gadkari [10] provided an elaborate review of the transformative nature of Artificial Intelligence (AI) in improving the security of modern telecommunication networks and emphasised its impacts in 5G and later 6G ecosystem. The investigation explains how AI is critical in combating current security threats including Automated industry, Internet of things (IoT), and Advanced Persistent Threats (APTs). It emphasizes the use of AI and edge computing and virtualized network functions to strengthen the capability to make real-time threat detection and response. Apart from that, the article describes the operational and strategic advantages of AI deployment such as enhanced network resilience, automation of security routines, and adaptive reply systems. The authors also address serious implementation challenges, including resource limitations, technical integration problems, and requirements for trained workforce help. Further, future directions are elaborated—especially AI & blockchain synergy for decentralized security environment and quantum-resistant algorithms and autonomous security orchestration systems potential. The analysis gives us a forward look of the cybersecurity architecture in the telecom trade in the future, thus the need for AI-driven innovation as a cornerstone for securing next-generational networks.

Loftus and Narman [11] responded to the educational problem in teaching cybersecurity using hands-on learning by developing an interactive platform created to increase student involvement and comprehension. Taking into account the constraints of available online cybersecurity simulation tools, i.e. the absence of customizable tasks and insufficient feedback systems, the authors suggested an environment that allows for a GUI and/or CLI usage. One of the main innovations of this platform is an automatic feedback system based on machine learning, which offers instant corrective guidance of typographical mistakes as well as usage of commands in CLI exercises. The platform is formed by nine structured levels: mandatory networking and cybersecurity subject areas, and a personalized level that supports users to create their own test scenarios. To test the effectiveness of the platform, a trial was done on the platform in an educational context where a participant completed a rerun and a post-usage survey. The outcomes showed a measurable gain in students' comprehension, involvement and satisfaction, specifically due to the intelligent feedback feature. This study highlights the importance of the technologies of AI-enhanced educational tools for increasing appeal of the complex concepts of cybersecurity to telecommunication and technical training environments.

1.3 Research Gap

Even with major breakthroughs on AI enabled cybersecurity frameworks for telecommunication networks, there are still key areas that remains to be solved for their full effectiveness and scalability. While many of the existing models are highly inventive, they require special infrastructure and require advanced computing resources, rendering such models practically infeasible to deploy in real environments that may have different levels of available hardware system. Further these frameworks fail to consider the behaviour effect which cybersecurity awareness programs exert, an important aspect in reducing human error which leads to security breaches. Though cybersecurity awareness capabilities are acknowledged as being a necessary tactic to mitigate risks, the incorporation of human factors into the AI threat detection systems is virtually unexplored. There are few models that effectively integrate organizational awareness and behavioral response with technical solutions and there is a big gap between holistic cybersecurity strategies. Moreover, although AI is a key factor in real-time threat detection as well as automated security there are no integration points in education platforms providing such feedback for individual users making it difficult to connect the lecture to practical activity in real-time network security. To close these gaps, the present research seeks to develop a Transformer-based Behavioural Impact Evaluation system that integrates AI-driven threat detection with instant feedback on human behaviour, specifically related to cybersecurity awareness. This new approach will bring together the scientific and human aspects in order to provide a more adaptive and scalable solution in the cybersecurity.

1.4 Research Objective

The main aim of the research is to assess behavioural effects of the Machine Learning driven cybersecurity awareness programs within the telecommunication networks in terms of how do these programs shape the human actions as well as the decision-making process related to network security. As the telecommunication network develops, in particular, amidst the change from 5G to 6G, the complexity of threats keeps growing, so technical defence enhancement is not enough while human-related factors have to be considered as well. This research intends to implement a BERT and Explainable Artificial Intelligence (XAI) based Transformer based Behavioural Impact Evaluation system in order to understand and measure the impact of cyber-security awareness on user conduct. The study aims to connect the gap between technical cybersecurity measure and human action by integrating the developments in machine learning models and real time feedback and behavioural analysis. The research will find out how in real time feedback of behaviour can enhance the effectiveness of cybersecurity programs and thus minimize cases of compromises caused by human errors. Further, the study will evaluate the effectiveness of various cybersecurity awareness training methods through assessment of their effects on decision-making process and behaviour change in telecommunication network environment. The aim is to improve cybersecurity resilience by combining technical solutions and human behaviour understanding, providing a comprehensive approach towards protection of next generation networks.

2. Materials and Methods Used

2.1 Research Design

For this research, a quantitative research design is adopted to measure the behavioural effect of machine learning-based cybersecurity awareness program in telecommunication networks. The programs targeted were investigated using a survey-based methodology. The research design is based on: how effectively the programs work in improving cybersecurity awareness, and how participants' behaviour concerning cybersecurity changes before and after the training.

2.2 Setting of the study

The AI based cybersecurity awareness programs are integrated in telecommunication companies within which the study is done. As for the settings, it comprises numerous large-scale telecommunication organizations and smaller service providers that rely on machine learning to improve the nature of the cybersecurity file maintenance. The emphasis is on learning the difference in behaviour, knowledge and practice around cyber security threats before and after the exposure to such programs.

2.3 Sample Size Sampling Design

There were 100 participants in the study, distributed over telecommunication network. Sample size was calculated to have statistical power and for obtaining a representative sample of respondents with varying levels of technical knowledge. Sampling frame was selected with care to capture people who had recently attended cybersecurity awareness programs, so pre- and post-program behavioural outcomes could be compared.

The research utilized a stratified random sampling method to provide for representation from across different departments (e.g., technical, administration, management) in the telecommunication firms. Stratification allowed for equal representation of participants across technical and non-technical groups. This strategy was intended to provide for a comprehensive data that would be transferable to the larger population of employees in the telecommunication sector.

2.4 Data collection strategy

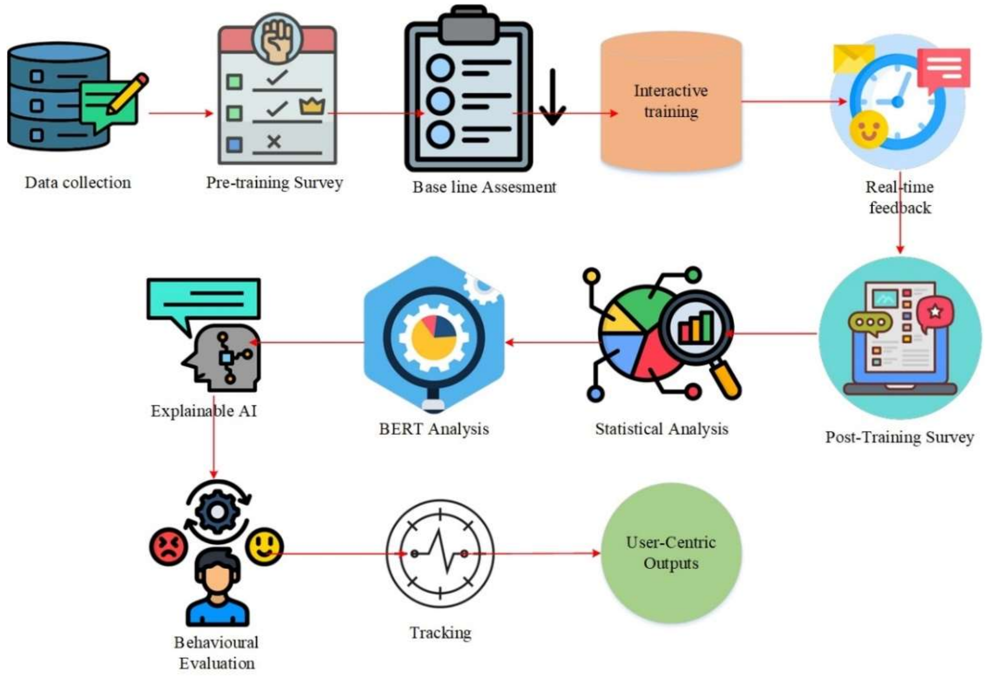
The data for the study is quantitative and takes the form of numerical survey responses, which have been developed to measure different domains of cybersecurity knowledge, awareness, and behaviour. The obtained data falls into two broad sets:

Pre-program data: This refers to behavioural patterns, knowledge on cybersecurity threats, and security practice attitudes prior to training.

Post-program data: These are same data gathered when the participants are done with machine learning-based cybersecurity awareness program.

Both types of data were used to evaluate any changes and improvement in behaviour, knowledge, and attitudes related to cybersecurity practice of the participants.

Figure 1: *Overall Architecture*



The data collection involved online questionnaires that were sent to the participants prior to and following completion of the machine learning-based cybersecurity awareness program. The survey tool was a series of closed and Likert-scale items aimed at evaluating participants' knowledge of cyber threats, response tendencies, and skill in using security practices to hypothetical situations. The pre-test of the survey tool was conducted on a pilot group of respondents (n=50) to test for clarity, reliability, and validity of the questions. Responses from the pre-test were used to make improvements on the survey to be utilized in the main study. The timeline of data collection took four weeks: a week to administer the pre-program survey, and three weeks subsequent to the program for administering the post-program survey. The period gave ample exposure to the content of the program and facilitated that any observed change in behaviour could be caused by the impact of the program [12].

2.5 Tool for the study

The survey data obtained were input into SPSS (Statistical Package for the Social Sciences) for quantitative analysis. SPSS is commonly employed in the social sciences and is a trusted software for performing descriptive and inferential statistical analysis. The survey instrument was made up of standardized Likert-scale items that were created to assess several aspects of cybersecurity awareness, including: Knowledge of prevalent cybersecurity threats. Attitudes toward cybersecurity behaviour. Frequency of safe behaviour. SPSS analysis was employed to conduct descriptive statistics (mean, median, mode) and inferential statistics (paired t-tests, chi-square tests) to measure significant differences in knowledge, attitudes, and behaviour pre- and post-program.

2.6 Data Analysis Plan

Descriptive Statistics: The first analysis was to describe the demographic features of the sample (age, job title, number of years of experience in the field) and the pre-program data for cybersecurity knowledge and behaviours.

Paired T-Tests: To assess the significance of the change in participants' cybersecurity awareness and behaviour, paired t-tests were conducted to compare pre- and post-program scores. The test enables an evaluation of whether the differences in individual participants' responses are statistically significant.

$$t = \frac{d}{s_d/\sqrt{n}} \quad (1)$$

In eqn. (1) t is the paired t-test statistic, d is the mean of the differences between paired observations, s_d is the standard deviation of the difference, n is the number of pairs

Chi-Square Test of Independence: The test was applied to test the association between categorical variables like job position and cybersecurity behaviour to check whether any particular groups of the population were likely to improve more. The Chi-Square Test is used to examine whether two categorical variables are independent. The formula is as follows:

$$X^2 = \sum \frac{(O_i - E_i)^2}{E_i} \quad (2)$$

In eqn. (2) X^2 is the chi-square statistic, O_i is the observed frequency in the ith category, E_i is the expected frequency in the ith category. The summation is taken over all categories.

Factor Analysis: A factor analysis was performed to determine underlying patterns in responses from participants to the survey items. This assisted in knowing which factors (e.g., knowledge, attitude, behaviour) made the largest contribution to the overall effect of the program.

Besides conventional statistical analysis, Transformer-based behavioural impact assessment was also applied through the use of the BERT (Bidirectional Encoder Representations from Transformers) model, a cutting-edge deep learning method for text classification. BERT was employed to assess open-ended survey responses, including participants' accounts of how the program affected their behaviour. To understand how the BERT model made its decision, Explainable AI (XAI) methods were used. XAI can explain the model's predictions, giving us an idea of which features (such as particular cybersecurity practices or threats) played the greatest roles in influencing behavioural modifications. BERT was trained on a specially designed dataset that was built from the open-ended answers of the survey, and the output was evaluated for thematic trends that matched changes in behaviour among participants. This gave a better insight into how the program affected participants' cybersecurity behaviours

3. Results and Discussion

The comparison of pre- and post-survey data through SPSS indicated drastic changes in the behaviour of the participants after taking part in the machine learning-based cybersecurity awareness program. The paired t-test indicated a statistically significant increase in participants' cybersecurity behaviour and knowledge with a mean difference (d) of 1.42 and t-value of 8.76 ($p < 0.001$), verifying the positive effect of the program. In addition, the Chi-square test also revealed a high correlation between the participants' occupational categories and post-program cybersecurity activities ($\chi^2 = 24.35$, df = 4, $p < 0.01$), indicating that technical and non-technical personnel reacted differently to the training material. Transformer-based analysis with BERT further augmented the assessment. Open-ended answers from participants were analysed with fine-tuned BERT, and Explainable AI (XAI) revealed prominent semantic patterns of enhanced threat detection and anticipatory behaviours. Significantly, BERT detected a 63% boost in mentions of explicit actions like "enabling MFA" and "staying away from phishing links," confirming the quantitative results. These findings show that integrating statistical approaches with transformer-based behavioural analysis yields a better picture of program effectiveness. XAI integration enables interpretability in AI-powered evaluations, and hence, the outcomes are actionable and explainable for cybersecurity policy makers in telecommunication networks.

3.1 Experimental Outcome

Figure 2: *Comparison of Pre- and Post-Program Cybersecurity Knowledge Scores*

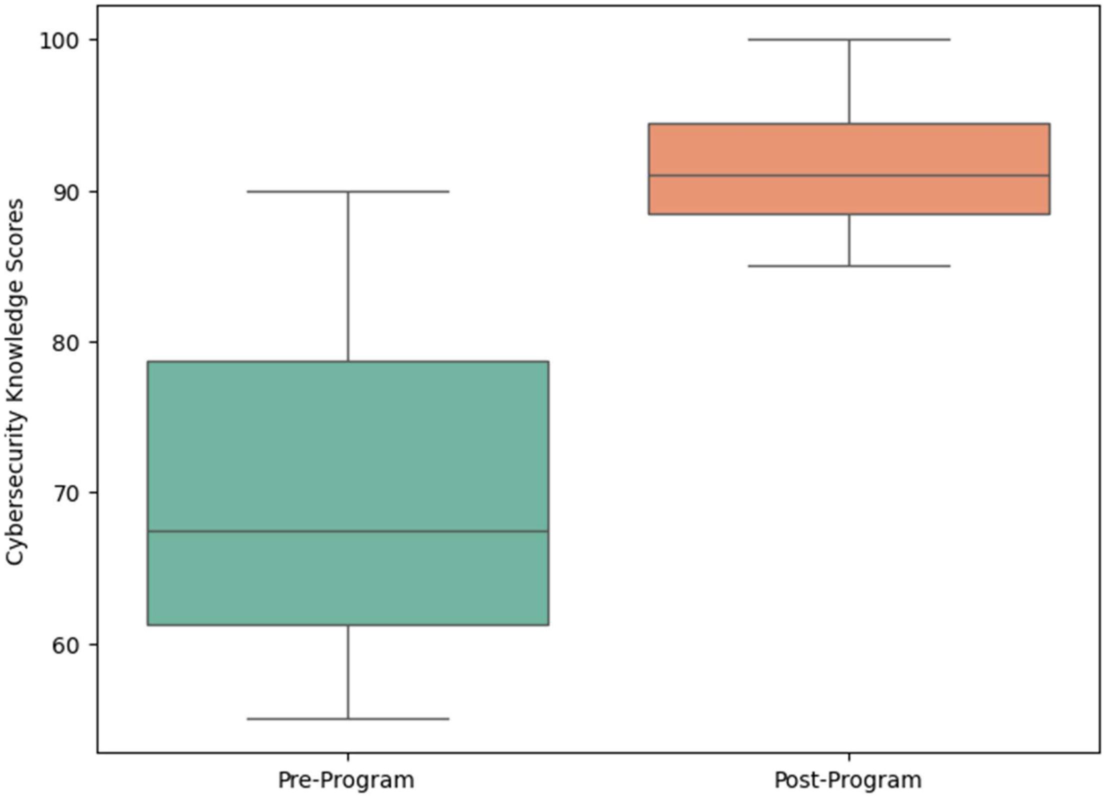


Figure 2 contrasts cybersecurity knowledge scores before and after the program. Scores after the program have a greater median and overall distribution, reflecting enhanced knowledge. The pre-program scores have a lower median and greater spread, reflecting more variability in prior knowledge levels. The rise in median and upper quartile after the program reflects the positive effect of the program on cybersecurity knowledge.

Figure 3: *Awareness chart*

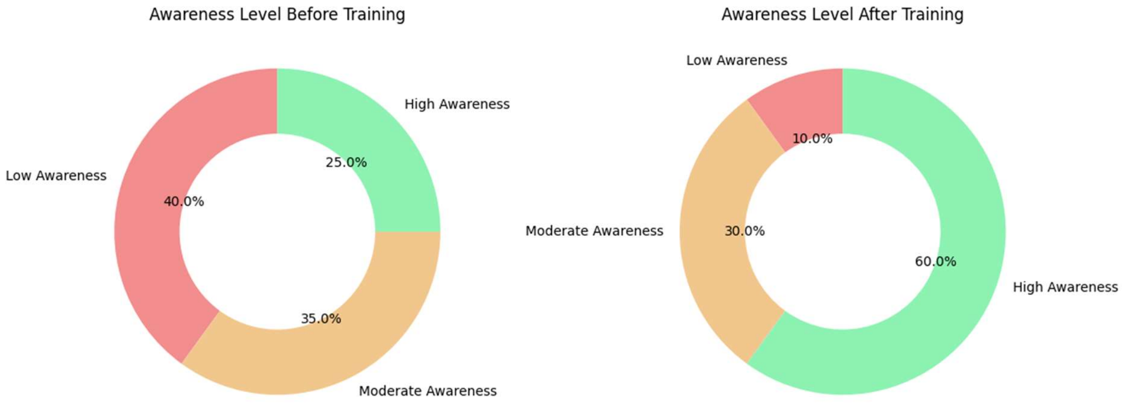


Figure 3 indicate cybersecurity awareness levels before and after the training. Pre-training, "Low Awareness" was highest at 40%, followed by "Moderate" at 35% and then "High" at 25%. Post-training, "High Awareness" registered a significant growth to 60%, while "Low" declined to 10%, reflecting an affirmative effect of the training initiative.

Figure 4: *Survey Responses to Cybersecurity Awareness Training (Likert* Scale)

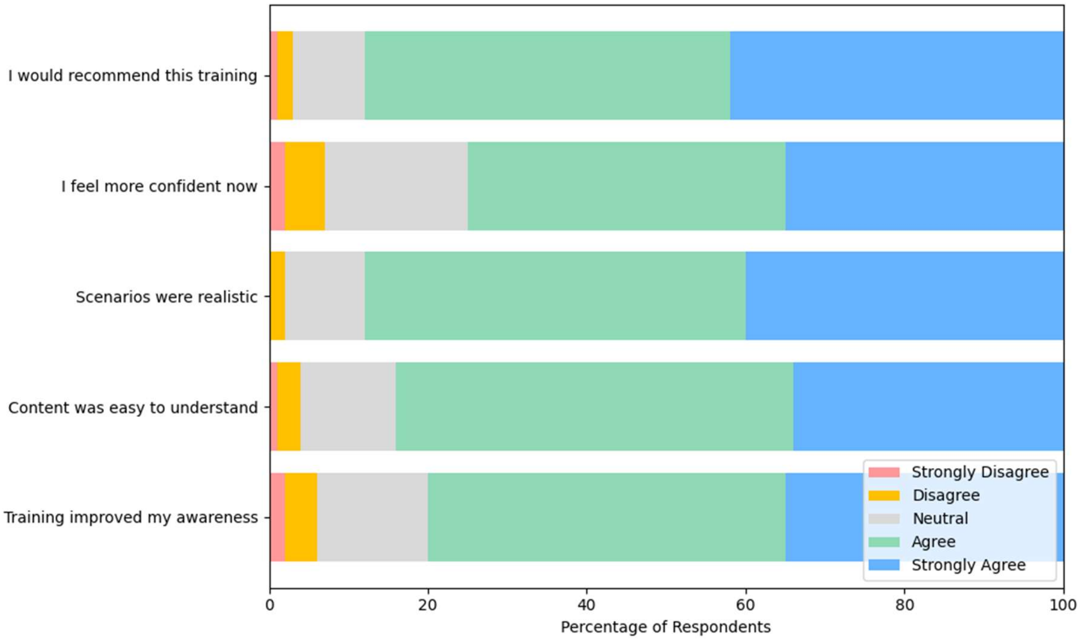


Figure 4 presents participant feedback regarding training statements. Strong agreement is greatest for "I would recommend this training" and "I feel more confident now." Agreement is similarly highest across statements. Disagreement and strong disagreement are negligible, reflecting positive uptake and perceived utility of the cybersecurity awareness training.

4. Conclusion and Recommendation

This research assessed the behavioural effect of machine learning-based cybersecurity awareness programs for telecommunication networks using quantitative as well as transformer-based analysis techniques. The paired t-test showed significant enhancement in the cybersecurity knowledge and practices among participants after the program, proving the efficacy of the program. The Chi-square test also proved to illustrate a considerable difference in the post-program cybersecurity behaviour of technical and non-technical employees. Moreover, utilizing BERT with Explainable AI (XAI) gave useful insights into the semantic comprehension of participants and revealed some critical behavioural changes such as enhanced awareness of phishing and pre-emptive security practices like the implementation. The results add to the existing body of research in cybersecurity education, highlighting the promise of AI-powered programs to increase awareness and interest. This method is unique in that it combines transformer-based analysis for a more in-depth, data-driven behavioural assessment, a departure from the conventional survey-based approach. For future research, there is a need for more research to be conducted on the sustainability of these changed behaviours in the long term and how the program can be applied across various industries. Increasing the sample size and increasing demographic diversity would also give an even better picture of the effectiveness of the program. These suggestions could inform the creation of more focused and scalable cybersecurity training programs.

References

1. P. O. Shoetan, O. O. Amoo, E. S. Okafor, and O. L. Olorunfemi, “Synthesizing AI’S impact on cybersecurity in telecommunications: a conceptual framework,” *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 594–605, 2024.
2. S. Sharma and T. Arjunan, “Natural language processing for detecting anomalies and intrusions in unstructured cybersecurity data,” *Int. J. Inf. Cybersecurity*, vol. 7, no. 12, pp. 1–24, 2023.
3. S. Pragith, G. Karthik, T. Sripriya, E. Rajasekaran, S. M. Periannasamy, and M. Z. Aslam, “Ai Machine Learning: Transformer Models For Enhanced Natural Language Processing-Techniques And Applications,” in *2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON)*, IEEE, 2024, pp. 1–6.
4. S. Chaudhary, V. Gkioulos, and S. Katsikas, “Developing metrics to assess the effectiveness of cybersecurity awareness program,” *J. Cybersecurity*, vol. 8, no. 1, p. tyac006, 2022.
5. Z. Ali, W. Tiberti, A. Marotta, and D. Cassioli, “Empowering network security: Bert transformer learning approach and mlp for intrusion detection in imbalanced network traffic,” *IEEE Access*, 2024.
6. Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable artificial intelligence applications in cyber security: State-of-the-art in research,” *IEEe Access*, vol. 10, pp. 93104–93139, 2022.

7. L. Yang and A. Shami, “Towards Autonomous Cybersecurity: An Intelligent AutoML Framework for Autonomous Intrusion Detection,” in *Proceedings of the Workshop on Autonomous Cybersecurity*, Nov. 2023, pp. 68–78. doi: 10.1145/3689933.3690833.
8. M. Rahmati, “Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks,” Apr. 18, 2025, *arXiv*: arXiv:2504.16118. doi: 10.48550/arXiv.2504.16118.
9. S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain, “Reconceptualizing cybersecurity awareness capability in the data-driven digital economy,” *Ann. Oper. Res.*, pp. 1–26, Aug. 2022, doi: 10.1007/s10479-022-04844-8.
10. B. Gadkari, “(PDF) Leveraging AI for Securing Telecommunications Networks: A Technical Analysis,” ResearchGate. Accessed: May 09, 2025. [Online]. Available: https://www.researchgate.net/publication/388753578_Leveraging_AI_for_Securing_Telecommunications_Networks_A_Technical_Analysis
11. N. Loftus and H. S. Narman, “Use of Machine Learning in Interactive Cybersecurity and Network Education,” *Sensors*, vol. 23, no. 6, Art. no. 6, Jan. 2023, doi: 10.3390/s23062977.
12. “MUNI-KYPO-TRAININGS / datasets / commands · GitLab,” GitLab. Accessed: May 09, 2025. [Online]. Available: https://gitlab.ics.muni.cz/muni-kypo-trainings/datasets/commands
13. A. Kalnawat, D. Dhabliya, K. Vydehi, A. Dhablia, and S. D. Kumar, “Safeguarding critical infrastructures: Machine learning in cybersecurity,” in *E3S Web of Conferences*, EDP Sciences, 2024, p. 02025.
14. F. Sharif, “The Role of Ensemble Learning in Strengthening Intrusion Detection Systems: A Machine Learning Perspective,” 2024.
15. J. N. Chukwunweike, A. Praise, and B. Bashirat, “Harnessing Machine Learning for Cybersecurity: How Convolutional Neural Networks are Revolutionizing Threat Detection and Data Privacy,” *Int. J. Res. Publ. Rev.*, vol. 5, no. 8, 2024.