Enhancing Cybersecurity Awareness Through Real-World Case Studies: A Data-Driven Evaluation of Training Effectiveness

Fabián Eduardo García Romero
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2025

Abstract *— Social engineering attacks have emerged as a dominant threat vector, bypassing technical defenses by exploiting human behavior. The study evaluates the effectiveness of real-world case study integration in cybersecurity training to strengthen awareness and user response. A mixed-methods approach, incorporating data-driven and scenario-based methodologies, was employed to measure user engagement, knowledge retention, and behavior change. Findings indicate that real case presentations significantly outperform traditional training by fostering deeper engagement, improving long-term awareness, and strengthening the human element in cybersecurity defense. The study contributes an adaptive, scalable educational framework that leverages real-world cases, interactive methods, and forward-looking technologies such as AI-driven simulations and behavior monitoring tools. Additionally, the proposed model aligns with evolving workforce competencies sought by public and private sector employers, offering a relevant, industry-informed solution to cybersecurity education. Integrating behavioral insights, real-world dynamics, and emerging technologies provides an innovative approach to preparing users to confront increasingly intricate cyber threats.*

Keywords *— Cybersecurity Awareness, Experiential Learning, Threat Recognition, Workforce Competencies*

INTRODUCTION

Social engineering remains a critical vulnerability in cybersecurity, consistently ranking among the top reported threats according to the FBI IC3 2024 Report [1]. These attacks, which exploit psychological manipulation rather than technical flaws, target individual behavior to bypass even the most advanced security systems. Despite significant investments in cybersecurity infrastructure, organizations continue to suffer breaches from phishing and impersonation tactics. Traditional training models, which are typically static, compliance-based, and theory-heavy, frequently fail to yield significant behavioral change or knowledge retention. These methods lack interactivity, practical application, and contextual relevance.

The FBI IC3 2024 Report documented more than 4.2 million complaints and $50.5 billion in financial losses over the past five years [1], highlighting the critical need to address human vulnerabilities in cybersecurity. These statistics highlight the need for training that incorporates behavioral insights. The report's increasing cybercrime complaints and losses supports the importance of enhanced awareness and adaptive learning frameworks in the current threat environment. The findings underscore the importance of implementing proactive measures to prevent cyber threats and protect individuals and organizations from financial harm.

The objective of this study is to evaluate the effectiveness of real-case cybersecurity training in enhancing threat recognition, knowledge retention, and behavioral resilience against social engineering attacks. The framework emphasizes user engagement, threat detection, and ongoing behavioral change by employing real-world case studies, interactive learning settings, and scenario-based assessments. The model seeks to conform to emerging workforce expectations, guaranteeing that cybersecurity awareness training is scalable and adaptable to changing threat environments. The framework highlights adaptive learning pathways to respond to emerging cyber threats and behavioral attack vectors.

LITERATURE REVIEW

Research studies like Aldawood and Skinner [2] emphasize persistent user awareness and preparedness gaps regarding phishing, vishing, and impersonation-based threats. Users often fail to recognize social engineering tactics, leading to successful breaches despite technological safeguards. Frameworks like the NIST Cybersecurity Framework [3] and Protection Motivation Theory (PMT) [4] stress that strengthening the human element through behavior-focused interventions is crucial for reducing vulnerabilities. Experiential learning, as outlined in Kolb's model [5], is recognized as a practical approach for promoting deeper engagement and long-term memory retention. Scenario-based learning has shown considerable promise in cybersecurity education, boosting knowledge retention, proactive behavior, and immediate threat recognition, as demonstrated by Ghosh and Francia [6]. Literature also suggests that integrating real-world cases and adaptive simulations enhances emotional engagement, fosters situational awareness, and encourages critical thinking, which is key to counteracting social engineering attacks. These findings collectively inform the development of the real-case training framework proposed in this study.

PROPOSED FRAMEWORK

The proposed framework integrates real-world case studies into cybersecurity training modules to address the gaps identified in traditional cybersecurity education. Grounded in experiential learning theory, it emphasizes active participation, reflection, and application of knowledge to reinforce understanding and retention. Participants engage in simulations that emulate authentic cyber threats, including phishing emails, vishing calls, and impersonation frauds, to cultivate practical threat identification and response skills. Behavioral analysis techniques monitor learners' decision-making processes and adapt scenarios to individual risk profiles, promoting personalized learning paths. The framework includes sequential modules beginning with introductory scenarios and gradually progressing to more complex, multi-layered attacks, ensuring a scalable and adaptive learning experience. The ultimate goal is to effectively prepare individuals to handle cybersecurity threats in real-world situations confidently.

The framework incorporates AI-driven adaptive learning platforms that dynamically tailor training difficulty and content based on learner performance. The approach ensures that individuals who quickly master basic concepts are challenged with advanced simulations, while those requiring additional practice receive targeted reinforcement activities. Feedback mechanisms are immediate and interactive, fostering a deeper learning process. Furthermore, integrating group-based exercises enhances collaborative problem-solving skills, mirroring real-world incident response teams. The comprehensive procedure aims to improve individual knowledge and resilience and build stronger, team-oriented cybersecurity cultures within organizations. The effectiveness of this framework is evaluated through a mixed-methods approach, assessing both quantitative performance metrics and qualitative user feedback.

The importance of transforming traditional cybersecurity awareness training methods is rooted in the evolving nature of cyber threats. Conventional approaches often rely heavily on theoretical content and infrequent training sessions, which lead to minimal retention and insufficient behavior change among participants. The dynamic threat landscape demands an educational model that adapts, engages, and empowers users to recognize and respond effectively to cyber threats. Proactively embedding real-world cases and interactive elements into the learning process, the proposed framework directly addresses these shortcomings, fostering practical skills and resilient cybersecurity behaviors that traditional methods fail to instill. As illustrated in Figure 1, modern training strategies such as immersive case studies, simulations, role-playing,

and gamification enhance knowledge retention, directly contributing to improved threat recognition and measurable behavioral change.

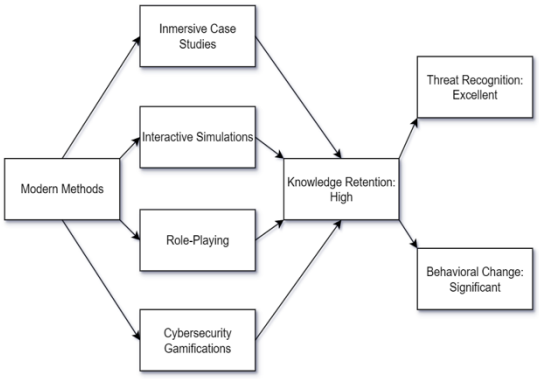

Figure 1
Modern Training Methods and Their Impact on Knowledge Retention

Cyber threats are becoming more sophisticated and frequent. Therefore, companies employ cybersecurity personnel with different skills. Technology is still important, but recent studies show an increasing need for non-technical knowledge, skills, and abilities (KSAs), including critical thinking, event analysis, communication, and social engineering awareness [7]. These include identifying and responding to real-world risks, communicating coherently across organizational levels, and adapting to dynamic threat situations. Private and public businesses increasingly want applicants with scenario-based decision-making and behavioral awareness. Real-world case studies, scenario-based exercises, and interactive simulations teach cybersecurity skills that are becoming increasingly important. These skills are crucial for individuals working in any role because all roles are significant to cybersecurity, as they are required to analyze complex situations, communicate effectively with team members, and stay ahead of constantly evolving threats. Systematically incorporating scenario-based decision-making and behavioral awareness training, organizations can ensure that their cybersecurity professionals are well-equipped to handle the challenges of today's digital landscape.

METHODOLOGY

The research applies a mixed-methods case study design to examine the effect of real-case presentations on cybersecurity awareness in a systematic way. The approach captures the best of both methods by integrating statistical analysis of training outcomes and profound qualitative insights derived from case narratives. The case study component facilitates an in-situ exploration of actual events and training activities. Each documented cybersecurity awareness activity or incident is considered a "case" for in-depth within-case analyses and cross-case comparisons.

In order to organize a comparative analysis between various cases, the research utilizes Qualitative Comparative Analysis (QCA) as a research instrument. QCA is a case-study approach that systematically examines cases to find patterns of conditions (training practices and contextual factors) linked with desired results. It successfully transforms qualitative case data into a form that has been analyzed across different cases. In essence, it enables the identification of intricate causal pathways that exist through numerous "routes" or combinations of factors that result in elevated levels of awareness. The combination of quantitative outcome measures and qualitative case pattern recognition provides a robust basis for evaluating the proposed cybersecurity awareness framework. In order to facilitate the mixed-methods case study analysis, secondary data collection procedures were undertaken, as outlined in the following subsection.

Data Collection Methods

Data for this study were collected from secondary sources, specifically publicly available datasets and published academic research. This approach allowed the research to cover various scenarios without the time and resource constraints associated with primary data collection while leveraging established knowledge in the field.

Quantitative data was obtained from public cybersecurity datasets, including repositories and databases containing information on training

outcomes, such as phishing email click-through rates, survey responses regarding awareness levels, and incident reporting rates following training interventions. Datasets were selected based on their relevance to training impact measurement, recency, and completeness. Metrics extracted included success rates of phishing simulations, security incident frequencies, and awareness program evaluation scores. Qualitative and additional quantitative insights were gathered through an extensive literature review. Academic studies, case reports, and meta-analyses were sourced from IEEE Xplore, ACM Digital Library, Statista, Google Scholar, ResearchGate, among other research papers.

Inclusion criteria focused on methodological rigor, alignment with research objectives, and the provision of comparative evaluations of different training approaches. Data points extracted from the literature included training types, content focus, evaluation methods, and reported outcomes. As the study relied exclusively on secondary data sources, no direct interaction with human subjects occurred, and therefore no additional ethical approval was required. Following data collection, the next methodological step involved developing the proposed educational framework.

Development of Educational Framework

As part of the methodological design, an educational framework for cybersecurity awareness training was developed based on insights from the comparative analysis and best practices identified in the literature. The framework was structured to bridge the gap between theoretical knowledge and practical application by incorporating realistic, engaging, and adaptable training content. It was designed as a guideline that organizations and educators could later adopt to strengthen their cybersecurity awareness initiatives.

- **Integration of Real-World Cases:** Training content was centered around real-world cybersecurity incidents, with each case study presenting context, progression, consequences, and lessons learned to enhance relevance and memorability.
- **Interactive Learning Methods:** The framework emphasized active engagement through discussions, role-playing, Q&A sessions, and simulations, fostering deeper cognitive processing and knowledge retention.
- **Reflection and Reinforcement:** Structured reflection activities, such as quizzes and scenario-based exercises, were incorporated to reinforce understanding and promote the practical application of learned concepts.
- **Adaptability and Currency:** The framework is designed to be regularly updated with emerging threat scenarios and tailored to different organizational contexts, sectors, and delivery formats.
- **Continuous Evaluation Mechanisms:** The framework included built-in feedback loops for assessing effectiveness through post-training surveys, behavioral observations, and incident monitoring, enabling continuous improvement.

This educational framework is the foundation for the case evaluations and effectiveness assessments, which are detailed in the subsequent sections. Figure 2 illustrates the design of the proposed cybersecurity awareness program, highlighting the integration of multiple instructional strategies. The model branches into four key components: continuous training through regular sessions, a hybrid delivery model combining online, in-person, and virtual instructor-led formats, the use of realistic scenario content based on real-world cyber incidents, and active participation through gamification methods like role-playing and simulations.

This diversified framework emphasizes that cybersecurity education should be flexible, immersive, and frequently reinforced to improve engagement, knowledge retention, and behavioral outcomes. Although resource-intensive methods such as simulations require greater investment, they offer significant benefits by fostering a security-conscious culture and reducing human error risks.

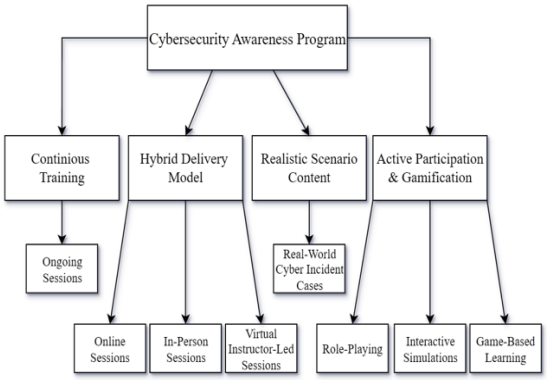

Figure 2
Cybersecurity Awareness Framework Diagram

IMPLEMENTATION

This section presents a theoretical implementation of the proposed cybersecurity awareness framework based on analyzing existing datasets and findings from prior research studies. The training framework was implemented in response to real-world cybersecurity incidents to ground learning in authentic scenarios. Each session featured a structured case study of an actual event detailing the attacker's methods, the breach impact, and the mitigation strategies. Research supports that examining real breaches enhances cybersecurity awareness more effectively than theoretical training and promotes better skill development and knowledge retention [9]. Practical case studies were selected based on conciseness, engaging yet factual narratives, memorable details, alignment with learning objectives, and contemporary relevance [9].

During sessions, facilitators introduced each case with contextual materials, such as news reports or investigation summaries, and used visual aids like screenshots or intrusion maps to enhance engagement. Open-ended questions were integrated throughout the presentation to stimulate critical thinking and personal application. This interactive storytelling approach leverages narrative techniques to strengthen participant connection to cybersecurity risks [10].

The framework's design also acknowledges the NIST Cybersecurity Framework (CSF), which outlines the core functions of Identify, Protect, Detect, Respond, and Recover. While traditional awareness training supports "Protect," real-case scenario-based training was implemented also to enhance organizational "Detect" and "Respond" capabilities [3]. To further illustrate the relevance of the proposed training framework, Table 1 maps the alignment between real-case scenario-based training and key functions of the NIST Cybersecurity Framework (NIST-CSF). This comparison highlights how realistic training methods directly support organizational goals in protecting, detecting, and responding to cyber threats.

Table 1
Real-Case Scenario and its Alignment with NIST-CSF

NIST CSF Function	Impact of Real-Case Scenario Training
Protect: Awareness/Training	Real-case scenarios satisfy the CSF's Protect role by showing users real-world assaults and hardening their defenses [3].
Detect: Anomalies & Events	In one year, staff taught on genuine phishing scenarios reported 66%, up from 7% [11].
Respond: Mitigate Impacts	An adaptive training approach reduced median phishing email "dwell time" by 32%, resulting in 1/3 faster employee response [11].

Several best practices were incorporated to ensure the framework's effectiveness during implementation, focusing on content relevance, customization, and active learner engagement. Best practices for rolling out the framework emphasized regularly updating training materials with recent incidents, tailoring modules to specific industry threats, and incorporating interactive elements that encourage reflection and discussion. The approach also recommended building a categorized library of case studies to enable training customization. Additionally, using brief, low-stakes assessments, real-world problem-solving activities, and periodic reinforcement sessions was identified as key to promoting long-term retention and more substantial behavioral change.

RESULTS

Key performance indicators (KPIs) were compared based on secondary data before and after similar interventions to evaluate the proposed real-world case-based training model's effectiveness. These indicators included phishing detection rates, knowledge retention, behavioral change, and participant engagement.

As illustrated in Figure 3, the model demonstrated substantial improvements across all metrics. Phishing detection accuracy increased from 30% to 80%, while knowledge retention rates rose from 20% to 75%. Similar gains were observed in behavioral change (30% to 80%) and participant engagement (40% to 85%). These results confirm that immersive, scenario-based education significantly enhances cybersecurity awareness and behavioral resilience. The improvements align with prior studies emphasizing the effectiveness of real-world case integration, gamification, and continuous engagement strategies for cybersecurity training [2],[11]–[14].

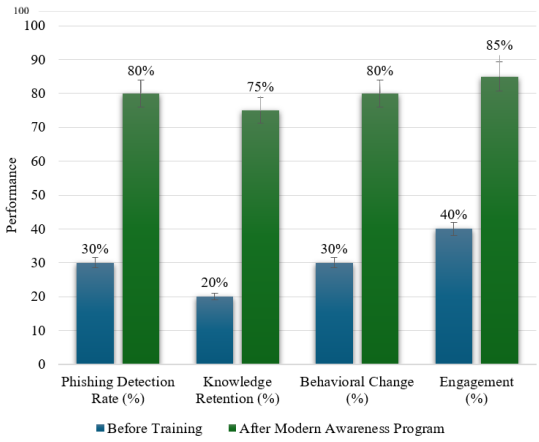

Figure 3
Impact of Real-Case Training on Cybersecurity Awareness Metrics

Performance comparison before and after implementing the modern cybersecurity awareness program across key indicators: phishing detection, knowledge retention, behavioral change, and engagement. These modeled outcomes were based on patterns identified from secondary datasets and prior research, demonstrating how the proposed educational framework can significantly enhance cybersecurity preparedness.

The comparison highlights the influence of different delivery methods and the integration of modern awareness programs on the effectiveness of cybersecurity awareness training. Incorporating real-world scenarios, hybrid delivery methods, and interactive learning improves cybersecurity awareness, behavior, and engagement outcomes. These results provide a solid foundation for further discussion regarding the implications, challenges, and recommendations for implementing the proposed framework in organizational settings.

DISCUSSION

The findings of this study reinforce important trends in cybersecurity awareness training practices. Analysis shows that comprehensive and continuous training programs have a substantial impact on user behavior, significantly reducing phishing failure rates and increasing proactive threat reporting. Integrating real-world case studies into training, such as videos illustrating phishing techniques or malware propagation, transforming abstract cybersecurity concepts into concrete, memorable learning experiences.

Moreover, cybersecurity training is increasingly shifting from a one-time annual event to an ongoing, iterative process. Evidence suggests that frequent interventions, including micro-trainings and monthly quizzes, support long-term knowledge retention and help build a "culture of cybersecurity" within organizations [15]. Leadership support for awareness initiatives is also growing, reflecting a broader institutional prioritization of cybersecurity education.

Effective training programs increasingly adopt a hybrid delivery model, combining online modules with in-person sessions to maximize flexibility, engagement, and effectiveness. The inclusion of realistic scenario content based on current attack trends further enhances relevance and retention [9]. In addition, embedding active participation methods, such as role-playing and gamified learning, has

proven to significantly improve motivation, knowledge retention, and behavioral change [16]. These findings highlight the importance of continuous, blended, interactive, and realistic training approaches in strengthening cybersecurity resilience across organizations.

The integration of Artificial Intelligence (AI) into cybersecurity awareness programs presents a major advancement for adaptability, personalization, and real-time threat detection. AI-driven applications such as adaptive phishing simulations, chatbots for learner support, and predictive analytics dashboards can tailor training content to individual behaviors, improving engagement and risk mitigation [17], [18]. Embedding AI technologies into the proposed real-case framework allows for dynamic scenario generation, automated learner guidance, customized feedback, and behavioral monitoring, all of which enhance the scalability and effectiveness of awareness initiatives. Through continuous analysis of user performance and threat trends, AI enables cybersecurity training to evolve responsively, reducing training fatigue and strengthening organizational resilience.

The article emphasizes the importance of changing cybersecurity awareness initiatives toward ongoing, real-world, and adaptive models. Organizations can more efficiently handle the rising complexity of cyber threats by combining case-based learning, interactive participation, hybrid delivery formats, and AI-driven improvements. Future training programs should emphasize personalization, continuous risk assessment, and dynamic content updates to preserve high degrees of user vigilance and security behavior across more varied and distributed workforces.

CONCLUSION

The research confirms that real-world case-based presentations and interactive instructional strategies substantially outperform traditional theoretical approaches in improving cybersecurity awareness. Scenario-driven training, immersive simulations, and gamified challenges led to greater knowledge retention, more substantial behavioral change, and heightened recognition of social engineering tactics compared to passive learning methods. Participants exposed to authentic breach scenarios demonstrated better decision-making and problem-solving skills, reinforcing the importance of active engagement and realistic content in cybersecurity education. These findings highlight that engaging, experiential learning strengthens the human element as the first defense against cyber threats.

Cybersecurity training programs must constantly change to meet new threats and change learning preferences in the future. While including regular updates, interactive activities, and real-world incident analysis, organizations should use dynamic, hybrid learning models that mix online flexibility with in-person interaction. Using artificial intelligence and other advanced, developing technologies will help to increase immersion and personalization even more. Companies can create a watchful, security-conscious workforce through the implementation of ongoing, realistic, interesting educational methods, therefore significantly lowering their vulnerability to cyber threats and supporting a proactive cybersecurity culture.

REFERENCES

[1] Internet Crime Complaint Center (IC3), *2024 Internet Crime Report*, Federal Bureau of Investigation, Washington, D.C., Rep. Apr. 23, 2025. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[2] H. Aldawood and G. Skinner, “Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues,” in *Future Internet*, vol. 11, no. 3, pp. 73, Mar. 2019. DOI: 10.3390/fi11030073.

[3] D. P. F. Möller, "NIST Cybersecurity Framework and MITRE Cybersecurity Criteria," in *Advances in Information Security*, 2023, pp. 231–271. DOI: 10.1007/978-3-031-26845-8_5.

[4] S. Sutton, "Health Behavior: Psychosocial theories," in *Elsevier eBooks*, 2001, pp. 6499–6506. DOI: 10.1016/b0-08-043076-7/03872-9.

[5] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*. Prentice Hall, 1984. [Online].

Available: https://www.researchgate.net/publication/235701029_Experiential_Learning_Experience_As_The_Source_Of_Learning_And_Development.

[6] T. Ghosh and G. Francia, "Assessing Competencies Using Scenario-Based Learning in Cybersecurity," in *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 539–552, Sep. 2021. DOI: 10.3390/jcp1040027.

[7] L. L. Sussman, "Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity hiring Managers," in *Journal of Higher Education Theory and Practice*, vol. 21, no. 6, Jul. 2021. DOI: 10.33423/jhetp.v21i6.4379.

[8] R. Chataut, P. K. Gyawali and Y. Usman, "Can AI Keep You Safe? A Study of Large Language Models for Phishing Detection," in *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2024, pp. 0548-0554. DOI: 10.1109/CCWC60891.2024.10427626.

[9] R. Bhaskar. (2022, May). *Better Cybersecurity Awareness Through Research*, *ISACA* (vol. 3) [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research.

[10] R. Knight and J. R. C. Nurse, "A Framework for Effective Corporate Communication after Cyber Security Incidents," in *Computers & Security*, vol. 99, p. 102036, Sep. 2020. DOI: 10.1016/j.cose.2020.102036.

[11] E. Baker. (2024, Jun. 13). *4 Essential Phishing Metrics to Reduce Risk* [Online]. Available: https://hoxhunt.com/blog/4-essential-phishing-metrics.

[12] E. Baker and M. Cartier. (2025). *Phishing Trends Report* [Online]. Available: https://hoxhunt.com/guide/phishing-trends-report.

[13] J. Huisman. (2024, June). *KnowBe4's 2024 Phishing by Industry Benchmarking Report Reveals that 34.3% of Untrained End Users Will Fail a Phishing Test* [Online]. Available: https://blog.knowbe4.com/knowbe4-2024-phishing-by-industry-benchmarking-report.

[14] Keepnet Labs. (2024, Nov. 12). *The Power of Gamification in Security Awareness Training* [Online]. Available: https://keepnetlabs.com/blog/the-power-of-gamification-in-security-awareness-training.

[15] L. Gallo *et al*., "The human factor in phishing: Collecting and analyzing user behavior when reading emails," in *Computers & Security*, vol. 139, pp. 103671, April 2024. DOI: 10.1016/j.cose.2023.103671.

[16] A. K. Gwenhure and F. S. Rahayu, "Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review," in *International Journal of Serious Games*, vol. 11, no. 1, pp. 83–99, Mar. 2024. DOI: 10.17083/ijsg.v11i1.719.

[17] S. O. Olabanji *et al.*, "AI-Driven Cloud Security: Examining the impact of user behavior analysis on threat detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 29, 2024. DOI: 10.9734/ajrcos/2024/v17i3424.

[18] A. Al-Subaiey *et al*., "Novel Interpretable and Robust Web-based AI Platform for Phishing Email Detection", Computers & Electrical Engineering, vol. 120, pp. 109625, May. 2024. DOI: 10.48550/arXiv.2405.11619