INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 1, (2026) E-ISSN: 2222-6990

# Enhancing Security Breach Awareness through Artificial Intelligence Tools

Maitha Musabah Salem Bin Dhawi Al Khateri, Diaya Ud Deen Deab Mahmoud Al Zitawi

Academy of Islamic Civilization, Faculty of Social and Islamic Sciences, Universiti Teknologi Malaysia, Malaysia

Email: musabahsalem@graduate.utm.my, diaya@utm.my

**DOI Link:** http://dx.doi.org/10.6007/IJARBSS/v16-i1/27326

***Published Date:*** 05 January 2026

**Abstract**

In light of the rapidly increasing cyber threats and the growing complexity of digital hacking methods, there has emerged a pressing need to develop security awareness approaches that go beyond traditional models. The research problem lies in the limited effectiveness of conventional awareness programs in addressing evolving cyber threats, particularly those resulting from the human factor, as well as their inability to adapt to users' behaviors and varying levels of awareness. This study aims to examine the role of artificial intelligence in enhancing the effectiveness of security breach awareness by exploring its capabilities in data analysis, risk prediction, and the personalization of awareness content in line with users' needs and security behaviors. The significance of this research stems from its contribution to supporting efforts to raise the level of cyber readiness among individuals and institutions and to enhance proactive responses to threats, in line with the requirements of cybersecurity in the digital age. The study adopted a descriptive analytical approach through reviewing and analyzing a set of relevant Arabic and international studies, with the aim of building a conceptual framework for an intelligent awareness model based on artificial intelligence tools. The results indicate that employing AI technologies such as machine learning, deep learning, and generative artificial intelligence effectively contributes to reducing security breaches related to the human factor, improving security decision-making, and increasing compliance with preventive measures. The study also concludes that intelligent awareness models are capable of providing proactive responses to cyber threats, despite the challenges associated with their use, most notably privacy concerns, algorithmic bias, and the need for clear legislative and ethical frameworks. This research offers a scientific vision that supports the adoption of intelligent awareness models as a strategic option within national and institutional cybersecurity strategies, emphasizing the importance of integrating technical, human, and organizational dimensions.

**Keywords:** Artificial Intelligence, Cybersecurity, Security Awareness, Security Breaches, Cybercrime, Human Factor, Digital Transformation, Intelligent Awareness Models

## Introduction

In recent years, the world has witnessed an unprecedented escalation in the pace of cyberattacks as a result of widespread digital transformation and the increasing reliance on electronic systems across vital sectors. This has made cybersecurity one of the most significant strategic challenges facing states, institutions, and individuals. Security breaches are no longer limited to traditional attacks; rather, they have evolved to include sophisticated intelligent attacks targeting information infrastructure and sensitive data, exploiting both technical and behavioral vulnerabilities of users.

In this context, artificial intelligence has emerged as one of the most important modern tools capable of creating a qualitative shift in cybersecurity, whether through early threat detection, prediction of future attacks, or analysis of attack patterns, thereby enhancing the effectiveness of defensive systems and reducing potential risks (Fadlallah, 2025; Ofusori et al., 2024).

Cybersecurity awareness is a fundamental pillar of digital protection systems. Numerous studies indicate that the human factor represents the weakest link in the cybersecurity chain due to lack of knowledge, insufficient training, or misuse of digital technologies. Hence, the importance of building effective awareness models based on artificial intelligence tools capable of analyzing user behavior, identifying knowledge gaps, and delivering tailored awareness content aligned with actual risk levels. These tools also contribute to enhancing rapid incident response, improving decision-making, and reducing cybercrime, which has become an increasing threat to national and economic security (Dahmani, 2023; Bakhoush, 2025).

With the rapid development of artificial intelligence technologies—including machine learning, deep learning, and generative AI—it has become possible to develop advanced awareness models capable of simulating cyberattacks, predicting hackers’ methods, and training users to handle potential threats through interactive and intelligent approaches. Recent studies confirm that employing these technologies in security awareness raises cyber readiness, reduces breach opportunities, and achieves an effective balance between technological advancement and security requirements (Benkmehdi & Saidi, 2022; Okdem & Okdem, 2024; Ferrag et al., 2024; Ndayipfukamiye et al., 2025).

## Artificial Intelligence And Its Role In Enhancing Cybersecurity Awareness

Artificial intelligence represents one of the most significant technological transformations reshaping cybersecurity concepts, particularly in awareness and prevention of security breaches. With the increasing complexity and stealth of cyberattacks, traditional awareness models are no longer sufficient. AI emerges as a strategic solution capable of analyzing vast volumes of security data, extracting attack patterns, and predicting potential risks before they occur, thereby fostering proactive cyber awareness among users and institutions alike (Fadlallah, 2025; Ofusori et al., 2024).

The importance of AI in cybersecurity awareness lies in its ability to shift from generic awareness approaches to personalized models based on analyzing users' digital behaviors. Machine learning and deep learning techniques enable understanding usage patterns, detecting unsafe behaviors, and identifying users' knowledge gaps, followed by delivering targeted awareness content aligned with real risk levels. Studies have shown that such intelligent awareness significantly reduces incidents caused by human error, which remains one of the primary causes of security breaches (Dahmani, 2023; Okdem & Okdem, 2024).

AI also plays a pivotal role in simulating cyberattacks as a training and awareness tool. Virtual scenarios can be created to simulate phishing attacks, malware, and ransomware, helping users recognize threats and respond effectively. This approach strengthens security culture and transforms awareness from theoretical guidance into an interactive, practice-based learning experience (Benkmehdi & Saidi, 2022; Ferrag et al., 2024).

Accordingly, integrating AI into security awareness programs is a fundamental step toward comprehensive cybersecurity, extending beyond technical threat detection to building users' behavioral and cognitive awareness, enhancing readiness, improving incident response, and reducing exploitation opportunities (Bakhoush, 2025; Ndayipfukamiye et al., 2025).

**A Model for Security Breach Awareness Using Artificial Intelligence Tools**

The proposed awareness model adopts a comprehensive approach that integrates technical and human dimensions, recognizing users as a core component of the security ecosystem. The model relies on analyzing the digital environment, monitoring potential threats, identifying target groups, and designing intelligent awareness programs based on data and automated analysis, thereby ensuring sustainable improvement in security awareness (Fadlallah, 2025; Ofusori et al., 2024).

The model utilizes AI techniques to collect and analyze data from previous cyber incidents, extract lessons learned, and employ them to develop proactive awareness content. It also allows continuous content updates in line with emerging threats, providing greater flexibility compared to traditional models. Studies confirm that AI-based models demonstrate higher adaptability to the rapidly evolving cyber threat landscape (Okdem & Okdem, 2024; Ferrag et al., 2024).

Furthermore, the model promotes continuous learning through interactive training programs that use intelligent assessment of users' awareness levels and provide immediate feedback to correct unsafe behaviors. This approach is critical in reducing breaches caused by negligence or lack of knowledge, which constitute a significant proportion of cyber incidents worldwide (Dahmani, 2023; Bakhoush, 2025).

Overall, the proposed model represents an integrated framework that combines intelligent analysis, interactive training, and personalized awareness, contributing to the development of a resilient security culture capable of addressing future challenges (Benkmehdi & Saidi, 2022; Ndayipfukamiye et al., 2025).

## Conclusion

The study concludes that the continuous rise in cyber threats necessitates the adoption of modern approaches that go beyond traditional protection methods. Artificial intelligence stands at the forefront as a strategic tool capable of enhancing cybersecurity effectiveness, particularly in awareness and prevention. The findings demonstrate that intelligent awareness models significantly raise users' security awareness and shift from reactive responses to proactive risk prediction and mitigation (Fadlallah, 2025; Ofusori et al., 2024).
The study also confirms that the human factor remains central to cybersecurity, either as a source of vulnerability or as an active protective element. AI-driven personalized awareness, based on behavioral analysis and continuous interaction, proves more effective than traditional programs by providing practical training and immediate feedback (Dahmani, 2023; Okdem & Okdem, 2024).

In light of technical, ethical, and legislative challenges, the success of AI-based awareness models depends on supportive regulatory environments, advanced digital infrastructure, and qualified human expertise. Achieving a balance between leveraging AI capabilities and protecting privacy and digital rights is essential for sustainable implementation (Benkmehdi & Saidi, 2022; Ferrag et al., 2024).

In conclusion, the AI-based security awareness model offers a promising framework for addressing contemporary cyber challenges and represents a critical step toward building a cybersecurity ecosystem grounded in awareness, continuous learning, and human–technology integration. The study recommends adopting this model within national and institutional cybersecurity strategies and supporting ongoing research and development to enhance digital trust in the era of accelerated digital transformation (Bakhoush, 2025; Ndayipfukamiye et al., 2025).

## References

Fadlallah, H. R. (2025). The role of artificial intelligence in enhancing the effectiveness of cybersecurity: An analytical study of challenges and future solutions. Egyptian Journal of Specialized Studies, 13(46.5), 1341–1362. https://doi.org/10.21608/ejos.2025.422622

Dahmani, M. (2023). Artificial intelligence as a mechanism for enhancing cybersecurity. Journal of Legal and Political Thought, 7(2), 597–608. Ammar Thleiji University of Laghouat, Algeria.

Benkmehdi, M., & Saidi, K. (2022). Artificial intelligence as an inevitable trend in protecting cybersecurity: The reality of today and the bet of tomorrow. ASJP – Articles Scientifiques et Publications, University of Algiers 3, Algeria.

Bakhoush, S. (2025). Artificial intelligence and cybersecurity: Functions and challenges. Algerian Journal of Human and Social Sciences, 9(1), 136–151.

Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial intelligence in cybersecurity: A comprehensive review and future direction. Applied Artificial Intelligence, 38(1), e2439609. https://doi.org/10.1080/08839514.2024.2439609

Okdem, S., & Okdem, S. (2024). Artificial intelligence in cybersecurity: A review and a case study. Applied Sciences, 14(22), 10487. https://doi.org/10.3390/app142210487

Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2024). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. arXiv. https://arxiv.org/abs/2405.12750

Ndayipfukamiye, T., Ding, J., Sarwatt, D. S., Philipo, A. G., & Ning, H. (2025). Adversarial defense in cybersecurity: A systematic review of GANs for threat detection and mitigation. arXiv. https://arxiv.org/abs/2509.20411