Online :ISSN 2964-1543

Global Social Science and Humanities Journal

gsshj.globaledupublisher.com

Global Education Publisher

The Role of Cybersecurity Awareness in Reducing the Complexity Impact of Authentication Methods on End-Users' Behavior

Abdulrahman Alsabri[1]*, Marwa Al-Hadi[2]

[1]Department of Information Systems, Faculty of Computer Science & IT , Sana'a University
[2]Department of Computer Science, Faculty of Computer Science & IT , Sana'a University

Corresponding Author email: abd.alsabri@su.edu.ye

Received: Aug 10, 2025
Revised : Oct 5, 2025
Accepted: Oct 25, 2025
Published : Nov 12, 2025

Abstract: As cyber threats continue to grow, organizations increasingly rely on complex authentication methods such as multi-factor authentication and biometric systems to protect sensitive information. Although these mechanisms strengthen security, many users experience them as difficult and disruptive, which can negatively influence compliance and everyday work practices. This study examines whether cybersecurity awareness can help reduce the perceived complexity of authentication methods and improve end-user behavior. Using a mixed-methods design, data were collected through a survey of 300 participants from different sectors, semi-structured interviews with 20 users, a controlled experiment, and a six-month follow-up study. The findings show that users who received cybersecurity awareness training reported lower levels of perceived complexity and higher compliance with authentication requirements than those without training. In particular, trained users demonstrated a noticeable improvement in their willingness to follow secure authentication procedures. Interview results further suggest that awareness programs help users better understand the purpose of security measures, reducing frustration and resistance. Overall, the study highlights the importance of human and behavioral factors in cybersecurity and shows that awareness initiatives can play a key role in improving both security practices and user experience.

Keywords: Cybersecurity awareness, authentication methods, end-user behavior, user experience , security training

1. Introduction

The rapid growth of digital technologies and online services has been accompanied by a corresponding rise in cybersecurity threats (Akram & Basit, 2023; Mallick & Nath, 2024). To

How to cite: Example Alsabri, A., & Al-Hadi, M. (2025). The Role of Cybersecurity Awareness in Reducing the Complexity Impact of Authentication Methods on End-Users' Behavior. Global Social Science and Humanities Journal, 3(4), 55–65. https://doi.org/10.59088/gi.v3i4.22

protect sensitive information and systems, organizations increasingly rely on advanced authentication mechanisms such as multi-factor authentication (MFA), biometric authentication, and adaptive authentication systems (Liao et al., 2021; Ametefe et al., 2024). These approaches provide stronger protection against unauthorized access and common attacks such as phishing, credential theft, and brute-force attempts (Oduri, 2024; Moustafa et al., 2021). However, despite their security benefits, such mechanisms are often perceived by users as complex and disruptive to everyday work activities (Mallick & Nath, 2024; Hemalatha, 2025).

The tension between security and usability has long been recognized as a central challenge in cybersecurity (Nielsen, 1994; Davis, 1989). While stronger authentication mechanisms improve protection, they frequently impose additional cognitive and procedural burdens on users. As a result, users may experience frustration, reduced productivity, and, in some cases, develop insecure coping behaviors such as reusing passwords, bypassing security steps, or disabling authentication features altogether (Oduri, 2024; Vardakis et al., 2024; Suru & Murano, 2019).

This challenge has become more pronounced in modern work environments where users are required to authenticate frequently, particularly in remote working, cloud-based systems, and mobile applications (Moustafa et al., 2021; Garg & Garg, 2024). In such contexts, the repeated use of complex authentication procedures can negatively affect user acceptance and compliance. Consequently, the effectiveness of authentication technologies depends not only on their technical robustness but also on how users perceive and interact with them (Liao et al., 2021; Zwilling et al., 2022).

Cybersecurity awareness has emerged as a promising approach to addressing this problem (Moustafa et al., 2021; Zwilling et al., 2022). Awareness programs aim to educate users about security risks, explain the purpose of authentication mechanisms, and provide guidance on how to use them correctly. Prior research suggests that informed users are more likely to adopt secure behaviors, show greater tolerance toward security controls, and comply with organizational security policies (Zwilling et al., 2022; Pramod, 2024). However, existing studies often focus on general security behavior and compliance, with limited attention given to how awareness influences users' perceptions of authentication complexity specifically (Goliath et al., 2024; Holden & Cetinkaya, 2024).

This study seeks to address this gap by examining the role of cybersecurity awareness in reducing the perceived complexity of authentication methods and shaping end-user behavior. By adopting a mixed-methods approach that combines survey data, interviews, experimental intervention, and longitudinal observation, the research provides a comprehensive analysis of how awareness training affects user perceptions, compliance, and behavioral change. The findings aim to contribute to a deeper understanding of the human factors involved in authentication systems and offer practical insights for organizations seeking to balance strong security with positive user experience.

2. Literature Review

2.1 Authentication Methods and Usability Challenges

Authentication mechanisms have evolved significantly as cyber threats have become more sophisticated. Traditional password-based systems, once considered sufficient, are now widely

regarded as inadequate due to their vulnerability to attacks such as phishing and credential reuse (Liao et al., 2021; Mallick & Nath, 2024). As a result, organizations increasingly adopt stronger authentication approaches, including multi-factor authentication (MFA), biometric systems, and adaptive authentication techniques (Ametefe et al., 2024; Fallahi et al., 2025). While these mechanisms enhance security, prior research consistently highlights their usability challenges. Users often perceive additional authentication steps as intrusive, time-consuming, and disruptive to workflow, which can negatively affect acceptance and satisfaction (Oduri, 2024; Hemalatha, 2025).

Human–computer interaction research emphasizes that security mechanisms that ignore usability principles may inadvertently increase risk by encouraging users to engage in insecure coping behaviors (Nielsen, 1994; Davis, 1989). This tension between security strength and ease of use remains a persistent challenge in authentication system design.

2.2 Impact of Authentication Complexity on End-User Behavior

Several studies have examined how the perceived complexity of authentication mechanisms influences user behavior. Research indicates that users confronted with complex authentication procedures often experience frustration, cognitive overload, and reduced productivity (Oduri, 2024; Vardakis et al., 2024). These experiences can lead to non-compliant behaviors such as password reuse, bypassing security steps, or disabling protective mechanisms altogether (Suru & Murano, 2019). Such behaviors undermine organizational security objectives and highlight the importance of considering human factors when implementing authentication systems. Contextual factors, including work environment and industry demands, further shape user responses to authentication complexity. For example, users operating in high-pressure sectors such as healthcare and finance may exhibit lower tolerance for complex security controls compared to users in more technically oriented environments (Garg & Garg, 2024). These findings suggest that authentication effectiveness depends not only on technical robustness but also on how users perceive and interact with security measures in their daily activities.

2.3 Cybersecurity Awareness and User Compliance

Cybersecurity awareness has been widely recognized as a key strategy for improving user behavior and strengthening organizational security (Moustafa et al., 2021; Zwilling et al., 2022). Awareness programs aim to educate users about security risks, explain the rationale behind security controls, and provide guidance on correct usage. Empirical studies show that trained users demonstrate higher levels of compliance, improved security attitudes, and reduced engagement in risky behaviors (Pramod, 2024; Goliath et al., 2024). Recent research also highlights the importance of interactive and tailored training approaches, such as gamification and context-specific education, in enhancing engagement and knowledge retention (Ayeswarya & Singh, 2024; Holden & Cetinkaya, 2024). However, while the positive effects of awareness programs on general security behavior are well documented, fewer studies have specifically examined their role in shaping users' perceptions of authentication complexity. In particular, limited research has combined quantitative and qualitative methods to explore how awareness training influences both perceived difficulty and long-term behavioral change.

2.4 Research Gap

Although prior studies have addressed authentication usability and cybersecurity awareness independently, there remains a lack of integrated research examining how awareness initiatives mitigate the perceived complexity of authentication mechanisms and influence user compliance over time. This study addresses this gap by empirically investigating the relationship between cybersecurity awareness, perceived authentication complexity, and end-user behavior using a mixed-methods and longitudinal approach.

3. Research Methodology

3.1 Research Design

This study adopted a mixed-methods research design to examine the role of cybersecurity awareness in shaping users' perceptions of authentication complexity and their compliance behavior. By combining quantitative and qualitative approaches, the study aimed to capture both measurable behavioral patterns and in-depth user experiences. The research consisted of four components: a survey, semi-structured interviews, a controlled experiment, and a six-month longitudinal follow-up.

3.2 Participants and Sampling

A total of 300 end-users participated in the survey phase of the study. Participants were recruited from multiple sectors, including information technology, healthcare, finance, and education, to ensure diversity in professional background and system usage. Stratified random sampling was used based on industry type, job role (technical and non-technical), and organizational size. Gender balance was maintained, with equal representation of male and female participants.

Eligibility criteria required participants to have prior experience using at least one form of advanced authentication, such as multi-factor authentication or biometric systems.

3.3 Data Collection Methods

1. Survey

An online questionnaire was used to collect quantitative data on user demographics, perceived authentication complexity, cybersecurity awareness, and compliance behavior. Responses were measured using Likert-scale items. The survey was distributed online and remained open for four weeks.

2. Interviews

To gain deeper insight into user perceptions, semi-structured interviews were conducted with 20 survey participants. Interviewees were selected to represent different industries and experience levels. Each interview lasted approximately 30 minutes and focused on participants' experiences with authentication methods, perceived challenges, and the impact of cybersecurity awareness training. All interviews were recorded with participant consent and transcribed verbatim.

3.4 Controlled Experiment

A controlled experimental study was conducted to evaluate the impact of cybersecurity awareness training on user behavior. Participants were divided into three groups:

- **Group 1:** Basic awareness training (30 minutes)
- **Group 2:** Enhanced training (60 minutes with interactive elements)
- **Group 3:** Control group with no training

Participants' perceived authentication complexity and compliance behavior were measured before and after the intervention using standardized survey instruments. The experiment was conducted over a three-month period.

3.5 Longitudinal Follow-Up

To assess long-term effects, a subset of 100 participants was monitored over six months. Data were collected at three time points: baseline, three months, and six months. This approach allowed the study to evaluate whether changes in perception and behavior were sustained over time.

3.6 Data Analysis

Quantitative data were analyzed using SPSS software. Descriptive statistics were used to summarize participant characteristics and response patterns. Inferential analyses, including t-tests and ANOVA, were conducted to compare trained and untrained groups. Structural equation modeling was employed to examine relationships between cybersecurity awareness, perceived complexity, and compliance behavior.

Qualitative interview data were analyzed using thematic analysis. Transcripts were coded to identify recurring themes related to user perception, training effectiveness, and behavioral change.

3.7 Ethical Considerations

Participation in the study was voluntary. All participants were informed of the study's purpose and provided informed consent prior to data collection. Responses were anonymized, and all data were used solely for academic research purposes.

4. Results

4.1 Participant Characteristics

The final survey sample consisted of 300 participants, evenly distributed by gender (150 males and 150 females), with ages ranging from 18 to 55 years. Participants represented multiple professional sectors, including information technology (30%), healthcare (25%), finance (20%), education (15%), and other sectors (10%). The distribution of participants by gender and industry is summarized in **Table 1**, which shows balanced representation across sectors and supports the diversity of the study sample.

Table 1 Cross-Tabulation Of Gender By Industry

Industry	Male (n)	Female (n)	Total (n)
IT	45	45	90
Healthcare	40	35	75
Finance	35	25	60

Education	20	25	45
Other	10	20	30
Total	150	150	300

4.2 Perceptions of Authentication Complexity

Survey findings indicate that a substantial proportion of participants perceived advanced authentication mechanisms as complex. Approximately 65% of respondents reported that multi-factor authentication (MFA) was difficult to use, while 70% indicated that complex authentication processes disrupted their daily workflow. Overall satisfaction with current authentication methods remained moderate, with only 40% of participants expressing satisfaction. Regression analysis further revealed that prior cybersecurity awareness training and frequent interaction with authentication systems were associated with lower perceived complexity. These relationships are illustrated in **Figure 1**, which shows the impact of cybersecurity awareness on perceived authentication complexity.

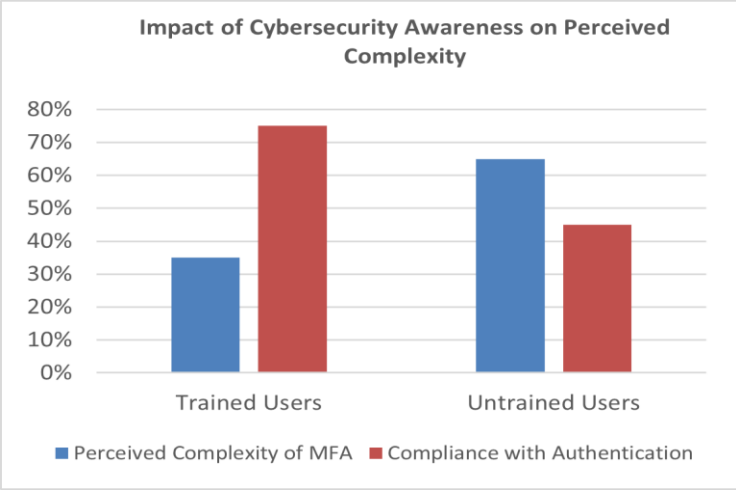

Figure 1. Impact of Cybersecurity Awareness on Perceived Complexity.

4.3 Impact of Cybersecurity Awareness Training

Cybersecurity awareness training had a noticeable positive effect on user perceptions and behavior. Participants who received training reported a 30% reduction in perceived authentication complexity compared to untrained users. In addition, compliance with authentication procedures was substantially higher among trained users (75%) than among untrained users (45%).

A comparison of trained and untrained users in terms of perceived complexity and compliance is presented in **Table 2**, clearly demonstrating the effectiveness of awareness training in improving both usability perceptions and secure behavior.

Table 2. Survey Results On Perceived Complexity And Compliance

Metric	Trained Users	Untrained Users
Perceived Complexity of MFA	35%	65%
Compliance with Authentication	75%	45%

4.4 Cross-Industry Differences

Differences in user perceptions were observed across industries. Participants from healthcare and finance sectors reported higher levels of frustration with complex authentication mechanisms compared to those working in information technology roles. However, the positive effects of cybersecurity awareness training were observed across all sectors, with the strongest compliance improvements reported in finance-related roles. These cross-industry variations are also reflected in **Figure 1**, which highlights sector-based differences in user responses.

4.5 Qualitative Interview Findings

Thematic analysis of the interview data identified three dominant themes: perceived complexity, training effectiveness, and behavioral change. A summary of these themes, along with representative participant quotes, is provided in **Table 3**. Prior to training, most participants described authentication procedures as cognitively demanding and disruptive. After participating in awareness sessions, interviewees reported improved understanding of security requirements and greater willingness to comply with authentication policies.

Table 3. Key Themes From Interviews

Theme	Frequency	Example Quote
Perceived Complexity	15/20	″ MFA feels like an extra step that slows me down.″
Training Effectiveness	18/20	″ Training helped me understand why MFA is needed.″
Behavioral Changes	16/20	″ I no longer disable MFA after the training.″

4.6 Longitudinal Findings

Longitudinal analysis of data collected over six months showed that improvements in perceived complexity and compliance were largely sustained over time. Although a slight decline in compliance was observed at the six-month mark, trained participants continued to demonstrate higher adherence to authentication protocols compared to untrained users.

5. Discussion

The findings of this study highlight the important role of cybersecurity awareness in shaping how users perceive and respond to complex authentication mechanisms. As organizations increasingly adopt advanced authentication methods such as multi-factor authentication and biometrics, usability concerns continue to influence user acceptance and compliance. The results

confirm that authentication complexity is not merely a technical issue but a behavioral and perceptual one, strongly influenced by users' understanding and awareness.

The quantitative results demonstrate that users who received cybersecurity awareness training reported significantly lower levels of perceived authentication complexity and higher compliance with security procedures than untrained users. These findings align with prior research suggesting that informed users are more likely to tolerate security controls and adhere to organizational policies. Importantly, this study extends existing work by showing that awareness training does not only improve general security behavior but also directly reduces users' perceptions of authentication difficulty.

The qualitative interview findings further support this interpretation. Participants frequently described feelings of frustration and cognitive burden when interacting with complex authentication systems prior to training. After participating in awareness sessions, many users reported a clearer understanding of the purpose behind authentication measures, which reduced resistance and improved acceptance. This suggests that awareness initiatives can help bridge the gap between security requirements and user experience by contextualizing security measures rather than presenting them as obstacles.

Cross-industry differences observed in the results indicate that contextual factors play a role in shaping user perceptions. Participants from high-pressure sectors such as healthcare and finance exhibited lower tolerance for authentication complexity, likely due to workflow demands and time constraints. Nevertheless, awareness training produced positive effects across all sectors, suggesting that education can partially offset contextual challenges when appropriately designed.

The longitudinal findings provide further insight into the sustainability of awareness interventions. While a slight decline in compliance was observed over time, trained users consistently demonstrated higher adherence levels than untrained participants. This indicates that awareness programs can have lasting benefits, although periodic reinforcement may be necessary to maintain their effectiveness in the long term.

From a social and behavioral perspective, these findings reinforce the importance of human-centered approaches to cybersecurity. Technical solutions alone are insufficient if users do not understand or accept them. Integrating awareness initiatives into organizational security strategies can help promote a culture of shared responsibility, where users actively participate in protecting digital assets rather than viewing security as an imposed burden.

6. Conclusion

This study examined the role of cybersecurity awareness in reducing the perceived complexity of authentication methods and improving end-user behavior. As organizations increasingly rely on advanced authentication mechanisms such as multi-factor authentication and biometric systems, usability challenges have emerged as a key factor influencing user acceptance and compliance. The findings of this research demonstrate that cybersecurity awareness plays a meaningful role in addressing these challenges by helping users better understand the purpose and value of security controls.

Results from the survey, controlled experiment, interviews, and longitudinal analysis consistently show that users who received awareness training reported lower levels of perceived authentication complexity and higher compliance with organizational security requirements. These outcomes suggest that awareness initiatives can mitigate frustration, reduce insecure coping behaviors, and encourage more positive engagement with authentication technologies. Importantly, the study highlights that security effectiveness depends not only on technical solutions but also on users' perceptions, knowledge, and attitudes.

From a broader perspective, this research contributes to the growing body of social and behavioral cybersecurity literature by emphasizing the human dimension of authentication systems. By integrating awareness programs into cybersecurity strategies, organizations can achieve a more balanced approach that supports both strong security and a positive user experience.

7. Future Work

While this study provides valuable insights, several directions for future research remain. First, future studies could examine the long-term effects of cybersecurity awareness programs over extended periods to determine whether observed behavioral improvements are sustained beyond six months. Longitudinal research across multiple years would offer deeper understanding of habit formation and training retention.

Second, cross-cultural and cross-organizational studies could explore how cultural norms, organizational size, and regulatory environments influence the effectiveness of awareness initiatives. Such work would help determine whether training strategies should be adapted to different social and institutional contexts.

Finally, future research could investigate the role of emerging authentication technologies—such as passwordless authentication and behavioral biometrics—and assess how awareness training can support user acceptance of these systems. Exploring interactive and adaptive training approaches, including gamified and personalized learning, may further enhance the effectiveness of cybersecurity awareness programs.

Funding

The work did not receive any kind of funding.

Conflicts of Interest

No Conflicts of interest

References

Akram, E., & Basit, F. (2023). *AI-powered information security: Innovations in cyber defense for cloud and network infrastructure*.

Ametefe, D. S., et al. (2024). Enhancing fingerprint authentication: A systematic review of liveness detection methods against presentation attacks. *Journal of The Institution of Engineers (India): Series B, 105*(5), 1451–1467.

Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access*.

Al Ansari, M. J., Al Ahmed, Y., & El Bahnaswi, H. H. (2024). Balancing usability and protection in AI and data security: A human-centric approach. In *2024 11th International Conference on Software Defined Systems (SDS)* (pp. 80–88). IEEE.

Al-Dhamari, N., & Clarke, N. (2024). GPT-enabled cybersecurity training: A tailored approach for effective awareness. In *IFIP World Conference on Information Security Education* (pp. 3–20). Springer.

Bedewy, S. F. (2024). The impact of data security and privacy concerns on the implementation of integrated smart cities. In *Foundations and perspectives* (Vol. 59).

Davies, A. J., & Krame, G. (2024). Measuring the level of fidelity required for transfer of learning in simulation-based learning exercises for novice and experienced practitioners. *Simulation & Gaming, 55*(4), 685–715.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Dehling, F., Tolsdorf, J., Federrath, H., & Iacono, L. L. (2024). Internet users' willingness to disclose biometric data for continuous online account protection: An empirical investigation. *Proceedings on Privacy Enhancing Technologies*.

Elkhodr, M., & Gide, E. (2025). Integrating generative AI in cybersecurity education: Case study insights on pedagogical strategies, critical thinking, and responsible AI use. *arXiv*. https://arxiv.org/abs/2502.15357

Fallahi, M., Arias-Cabarcos, P., & Strufe, T. (2025). On the usability of next-generation authentication: A study on eye movement and brainwave-based mechanisms. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (pp. 1–14).

Garg, G., & Garg, A. (2024). *Decentralized authentication: Approaches, comparative study, and future trends*.

Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. *arXiv*. https://arxiv.org/abs/2411.03219

Hemalatha, T. (2025). Usability challenges in biometric systems: False rejections and user frustration. In *The future of digitalization: Crafting exceptional user experiences in biometric contactless payment systems* (p. 97).

Holden, J., & Cetinkaya, D. (2024). *Using personalised authentication flows to address issues with traditional authentication methods*.

Kumar, T., Bhushan, S., Sharma, P., & Garg, V. (2024). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In *Leveraging computer vision to biometric applications* (pp. 34–67). Chapman and Hall/CRC.

Liao, Z., Pang, X., Zhang, J., Xiong, B., & Wang, J. (2021). Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey. *IEEE Transactions on Network and Service Management, 19*(2), 1159–1175.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News, 190*(1), 1–69.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology, 12*, 561011.

Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann.

Nandan Prasad, A. (2024). Regulatory compliance and risk management. In *Introduction to data governance for machine learning systems: Fundamental principles, critical practices, and future trends* (pp. 485–624). Springer.

Oduri, S. (2024). Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era. *International Journal of Innovative Research in Science Engineering and Technology, 13*(7), 13632–13640.

Pramod, D. (2024). Gamification in cybersecurity education: A state of the art review and research agenda. *Journal of Applied Research in Higher Education*.

Qin, D., Amariucai, G., Qiao, D., & Guan, Y. (2024). Improving behavior-based authentication against adversarial attack using XAI. *arXiv*. https://arxiv.org/abs/2402.16430

Shethiya, A. S. (2024). AI-enhanced biometric authentication: Improving network security with deep learning. *Academia Nexus Journal, 3*(1).

Suru, H. U., & Murano, P. (2019). Security and user interface usability of graphical authentication systems: A review. *International Journal of Engineering Trends and Technology, 67*, 17–36.

Tsaliki, K. C. (2024.). Revolutionizing identity management with AI: Enhancing cyber security and preventing ATO. *International Research Journal of Modernization in Engineering Technology and Science, 6*.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the internet of things. *Electronics, 13*(16), 3343.

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *PLOS ONE, 19*(10), e0312266.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97.