The OSCAR PUBLISHING Services
International Journal of Pedagogics

VOLUME Vol.06 Issue04 2026
PAGE NO. 255-259
DOI 10.37547/ijp/Volume06Issue04-58

Teaching "Fundamentals of Information Security" In An E-Learning Environment: Relevance, Challenges, And Outcomes

Sherzod Mavlonov
Department of Information Technologies, Gulistan State University, Gulistan, Uzbekistan

Received: 05 March 2026; **Accepted:** 29 March 2026; **Published:** 22 April 2026

Abstract: The rapid advancement of digital technologies has made information security a critical competency for students across numerous disciplines. This study investigates the relevance and effectiveness of teaching the course "Fundamentals of Information Security" within an e-learning environment. A mixed-methods approach was employed, involving 186 undergraduate students from three universities in Uzbekistan over one academic semester (2024–2025, 2026–2026). Quantitative data were gathered through pre- and post-course assessments, while qualitative insights were collected via structured interviews and reflective surveys. Results indicate a statistically significant improvement in student knowledge ($p < 0.001$), with mean scores rising from 43.2% to 78.6%. Students demonstrated enhanced awareness of cyber threats, encryption principles, and secure network practices. The e-learning format facilitated flexible access, self-paced learning, and the integration of interactive simulations unavailable in conventional classrooms. Key challenges identified included digital divide issues, student motivation without physical supervision, and the need for continuous content updating to reflect evolving threats. The study concludes that e-learning is not only a viable but also an increasingly necessary modality for delivering information security education, particularly in developing economies undergoing digital transformation.

Keywords: Information security education, e-learning, cybersecurity, online learning, digital literacy, Uzbekistan, higher education.

Introduction: The global transition toward digitally mediated education, accelerated by the COVID-19 pandemic, has fundamentally reshaped instructional delivery across academic disciplines [1]. Among these disciplines, information security—once confined to niche technical programs—has emerged as a universally relevant field of study. As societies become increasingly dependent on interconnected digital infrastructure, the risks posed by cyberattacks, data breaches, and social engineering have expanded beyond technical specialists to affect individuals, businesses, and governments alike [2].

In Uzbekistan, as in many Central Asian countries, the national digital transformation agenda has intensified the demand for graduates possessing foundational cybersecurity competencies [3]. The government's "Digital Uzbekistan 2030" strategy explicitly identifies the development of information security expertise as a strategic priority, placing higher education institutions under pressure to produce graduates capable of securing digital systems and infrastructure [4].

E-learning, broadly defined as the use of digital technologies to deliver educational content and facilitate learning interactions, offers a compelling response to these demands [5]. It provides scalable, geographically unbounded access to educational resources, enables self-paced and adaptive learning pathways, and supports multimedia-rich instructional experiences. However, its effectiveness depends on multiple factors, including pedagogical design, technological infrastructure, learner readiness, and the nature of the subject matter itself [6].

Information security as a discipline presents unique characteristics that make its e-learning delivery both

promising and challenging. The field is inherently dynamic: threat landscapes evolve continuously, requiring instructional content to be updated regularly. Moreover, effective security education requires not only declarative knowledge but also procedural skills—such as configuring firewalls, analyzing network traffic, or implementing cryptographic protocols—that traditionally demand hands-on laboratory practice [7].

Despite the growing importance of this intersection, empirical research examining the outcomes of teaching information security through e-learning platforms—particularly in Central Asian higher education contexts—remains limited. This study addresses that gap by investigating the relevance, pedagogical effectiveness, and practical challenges associated with delivering the "Fundamentals of Information Security" course through an e-learning environment in Uzbekistan.

The primary research questions guiding this study are: (1) To what extent does e-learning delivery of information security content lead to measurable gains in student knowledge? (2) What factors facilitate or impede effective learning in this context? (3) How do students perceive the relevance and quality of e-learning instruction in information security?

METHODS

This study adopted a concurrent mixed-methods design, integrating quantitative assessment data with qualitative interview and survey data to provide a comprehensive picture of e-learning outcomes in information security education [8].

1 Participants

A total of 186 undergraduate students (114 male, 72 female; mean age = 20.3 years, SD = 1.7) enrolled in the "Fundamentals of Information Security" course at three universities in Uzbekistan participated in the study during the 2024–2025, 2025-2026 academic years. Participants were drawn from computer science, information systems, and applied mathematics programs. Informed consent was obtained from all participants, and the study received ethical clearance from the institutional review boards of all three participating institutions.

2 Course Structure and E-Learning Platform

The course was delivered over 16 weeks via the Moodle learning management system, supplemented by a locally hosted virtual laboratory environment. The curriculum covered seven thematic modules: (1) introduction to information security concepts and terminology; (2) cryptography and encryption methods; (3) network security and protocols; (4) authentication and access control mechanisms; (5) vulnerability assessment and ethical hacking fundamentals; (6) security policies and regulatory frameworks; and (7) emerging threats and incident response. Each module included recorded video lectures (15–25 minutes each), required readings, interactive quizzes, discussion forums, and at least one virtual lab exercise. Live synchronous sessions were held bi-weekly via Zoom for Q&A and case study discussions.

3 Data Collection

Quantitative data were collected through a validated 50-item knowledge assessment administered before the course began (pre-test) and at its conclusion (post-test). Items covered all seven modules and were reviewed by a panel of three cybersecurity experts for content validity. Internal consistency of the instrument was confirmed with a Cronbach's alpha of 0.84. Additionally, students completed a 20-item Likert-scale course satisfaction survey at the end of the semester, measuring perceived content relevance, instructional quality, platform usability, and overall satisfaction. Qualitative data were gathered through semi-structured interviews conducted with a purposively selected subsample of 24 participants, representing a range of academic performance levels and demographic characteristics. Interviews lasted 30–45 minutes and were audio-recorded and transcribed verbatim.

4 Data Analysis

Quantitative data were analyzed using IBM SPSS Statistics 27. A paired-samples t-test was used to evaluate pre- to post-test knowledge gains. Descriptive statistics were calculated for satisfaction survey items. Cohen's d was computed to estimate effect size. Qualitative interview transcripts were analyzed using thematic analysis following Braun and Clarke's six-phase framework [9], with two independent coders achieving a Cohen's kappa of 0.81, indicating strong inter-rater reliability.

RESULTS

1 Knowledge Gains

Students demonstrated statistically significant improvement in information security knowledge from pre-test to post-test. The mean pre-test score was 43.2% (SD = 9.8%), which increased to 78.6% (SD = 8.3%) at post-test. A paired-samples t-test confirmed that this improvement was statistically significant ($t(185) = 41.7$, $p < 0.001$), with a large effect size ($d = 3.06$). The greatest knowledge gains were observed in the modules on cryptography (+42.1 percentage points) and authentication mechanisms (+39.7 percentage points), while the module on regulatory frameworks showed the smallest but still significant gain (+22.4 percentage points).

Table 1. Pre- and Post-Test Scores by Module

Module	Pre-test (%)	Post-test (%)	Gain (pp)
Introduction to IS concepts	46.1	79.4	+33.3
Cryptography and encryption	38.5	80.6	+42.1
Network security	44.2	81.3	+37.1
Authentication and access control	39.8	79.5	+39.7
Vulnerability assessment	42.6	77.1	+34.5
Security policies and regulation	51.3	73.7	+22.4
Emerging threats and response	40.9	78.2	+37.3
Overall	43.2	78.6	+35.4

2 Student Satisfaction

Satisfaction survey results were generally positive. On a five-point Likert scale, students rated content relevance highest ($M = 4.31$, $SD = 0.62$), followed by perceived usefulness of virtual labs ($M = 4.18$, $SD = 0.74$), and platform usability ($M = 3.97$, $SD = 0.81$). The lowest-rated dimension was timeliness of instructor feedback ($M = 3.52$, $SD = 0.93$), reflecting students' desire for more immediate responses in the asynchronous environment. Overall course satisfaction averaged 4.07 out of 5.00 ($SD = 0.68$).

3 Qualitative Findings

Thematic analysis of interview data produced four primary themes: (i) Perceived Relevance and Career Significance — the majority of students (20/24) articulated a clear connection between course content and their anticipated professional roles, with several noting that awareness of current cyber threats heightened their motivation; (ii) Value of Interactive and Simulated Learning — virtual lab exercises were consistently highlighted as the most engaging and pedagogically valuable component, with students describing the ability to practise configuring network security settings in a consequence-free environment as "irreplaceable"; (iii) Self-Regulation Challenges — twelve participants acknowledged difficulties maintaining consistent study schedules without the structure of in-person classes, and five reported episodes of prolonged disengagement; (iv) Infrastructure and Connectivity Barriers — eight students reported intermittent internet connectivity as a significant obstacle, particularly those residing in rural or peri-urban areas.

DISCUSSION

The findings of this study provide robust empirical support for the effectiveness and relevance of delivering "Fundamentals of Information Security" through an e-learning environment. The magnitude of knowledge gains (mean increase of 35.4 percentage points; $d = 3.06$) substantially exceeds benchmarks reported in comparable studies of traditional classroom-based information security instruction [10, 11], suggesting that the affordances of e-learning—self-pacing, multimedia integration, and repeated access to recorded content—may be particularly well-suited to this domain.

The superior gains observed in cryptography and authentication modules are theoretically consistent with cognitive load theory [12]: these topics involve complex, layered conceptual structures that benefit

from the pause-and-replay functionality of asynchronous video lectures, as well as from interactive visualizations that are difficult to replicate on a physical whiteboard. Students' qualitative emphasis on virtual labs corroborates findings from prior research on cybersecurity simulation environments [13, 14], reinforcing the view that experiential digital practice is a critical success factor.

The relatively modest satisfaction with instructor feedback timeliness merits attention. Research in online education consistently identifies timely, individualized instructor feedback as one of the strongest predictors of student satisfaction and persistence [15]. In information security contexts, where students frequently encounter unfamiliar technical errors during lab exercises, delayed feedback may generate cognitive frustration that impedes learning. Institutions implementing this course should consider establishing guaranteed 24-hour response windows or deploying AI-assisted tutoring tools to supplement human instructor availability.

Self-regulation challenges identified in the qualitative data align with the broader e-learning literature, which recognizes metacognitive self-management as a decisive variable in online learning outcomes [16]. Students in developing economies may have had limited prior exposure to self-directed learning modalities, making explicit scaffolding of study habits—through learning contracts, automated progress reminders, or peer accountability structures—a valuable pedagogical investment.

The infrastructure barriers reported by rural students underscore a structural equity concern. While e-learning expands geographical access in principle, its benefits are contingent on reliable internet connectivity—a precondition that remains unevenly distributed in Uzbekistan [17]. Hybrid delivery models, offline-capable course modules, or mobile-optimized content could partially mitigate this disparity.

This study is subject to several limitations. The sample was drawn from three universities in a single country, limiting generalizability to other educational contexts. The absence of a matched control group receiving traditional instruction precludes causal attribution of gains exclusively to the e-learning format. Future research should employ randomized controlled designs and include longitudinal follow-up to assess the durability of knowledge gains and their transfer to professional practice.

CONCLUSION

This study demonstrates that teaching "Fundamentals of Information Security" in an e-learning environment is not only feasible but highly effective and increasingly necessary in the context of accelerating digital transformation. Students achieved significant, large-magnitude gains in information security knowledge, expressed positive evaluations of course relevance and virtual laboratory exercises, and identified clear connections between the course and their professional aspirations. Simultaneously, the study highlights persistent challenges related to self-regulation, feedback latency, and infrastructure equity that must be addressed through deliberate instructional design and institutional policy. As the global cybersecurity talent shortage continues to grow, e-learning platforms represent a scalable and democratizing vehicle for building the information security literacy that digital societies urgently require.

REFERENCES

1. Hodges, C., Moore, S., Lockee, B., Trust, T., & Bond, A. (2020). The difference between emergency remote teaching and online learning. EDUCAUSE Review, 27, 1–9.
2. Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004
3. Yusupov, B., & Mamatov, N. (2021). Digital transformation of education in Uzbekistan: Opportunities and challenges. Journal of Central Asian Studies in Education, 4(2), 12–24.
4. Ministry of Digital Technologies of Uzbekistan. (2020). Digital Uzbekistan 2030: Strategic roadmap. Tashkent: Government of the Republic of Uzbekistan.
5. Garrison, D. R. (2017). E-learning in the 21st century: A community of inquiry framework for research and practice (3rd ed.). Routledge.
6. Ally, M. (2019). Competency profile of the digital and online teacher in future education. International Review of Research in Open and

Distributed Learning, 20(2), 302–318. https://doi.org/10.19173/irrodl.v20i2.4206

7. Conklin, W. A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. Proceedings of the 39th Hawaii International Conference on System Sciences (pp. 1–10). IEEE.
8. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
9. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
10. Dark, M., Ekstrom, J., & Solworth, J. (2005). Integrating security in the computer science curriculum. ACM SIGCSE Bulletin, 37(4), 68–72. https://doi.org/10.1145/1113847.1113876
11. Mavlonov, S. H., & Orzuqulov, B. S. (2025). Teaching information security in distance education: methodological challenges and solutions. Теоретические аспекты становления педагогических наук, 4(10), 64-66.
12. Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4
13. Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. Proceedings of the 2011 International Conference on Security and Management (pp. 1–7). CSREA Press.
14. Tobarra, L., Robles-Gómez, A., Ros, S., Hernández, R., & Caminero, A. C. (2014). Analyzing the students' behavior and relevant topics in virtual learning communities. Computers in Human Behavior, 31, 659–669. https://doi.org/10.1016/j.chb.2013.10.001
15. Hattie, J., & Timperley, H. (2007). The power of feedback. Review of Educational Research, 77(1), 81–112. https://doi.org/10.3102/003465430298487
16. Zimmerman, B. J. (2002). Becoming a self-regulated learner: An overview. Theory Into Practice, 41(2), 64–70. https://doi.org/10.1207/s15430421tip4102_2
17. International Telecommunication Union. (2023). Measuring digital development: Facts and figures 2023. Geneva: ITU Publications.