

Article

Integrating Cybersecurity Education into University Mental Health Education: Values, Challenges, and Approaches

Jinshan Wu ^{1,*}
¹ Hainan Vocational University of Science and Technology, Haikou, China

* Correspondence: Jinshan Wu, Hainan Vocational University of Science and Technology, Haikou, China

Abstract: The rapid proliferation of digital technologies has fundamentally transformed the higher education landscape, necessitating innovative pedagogical strategies to safeguard student well-being. Integrating cybersecurity education into university mental health education not only addresses the evolving educational environment in the digital age but also provides a crucial new educational approach to enhance students' online adaptability, psychological resilience, and self-protection awareness against cyber threats. As students increasingly navigate complex digital ecosystems, the intersection of cyber risk and psychological vulnerability becomes more pronounced. Currently, however, this interdisciplinary integration faces significant systemic challenges. These include unclear educational positioning, inadequate institutional coordination mechanisms, insufficient faculty support and training, and outdated content formats that fail to adequately meet contemporary student needs, all of which severely hinder practical effectiveness. To overcome these barriers, this paper argues that universities must proactively advance practical efforts by clarifying overarching educational objectives and establishing robust operational frameworks. Furthermore, empowering educators through targeted professional development and innovating both curriculum content and delivery methods are essential steps. By implementing these strategies, higher education institutions can achieve an effective, synergistic alignment between cybersecurity education and mental health education in terms of goals, content, and pedagogical approaches. Ultimately, this comprehensive integration will support the holistic physical and mental development of college students while simultaneously driving the essential enhancement of their digital literacy and cyber resilience in an increasingly interconnected world.

Keywords: mental health education; cybersecurity education; college students; digital literacy; educational integration

1. Introduction

The "Outline for Building a Strong Education Nation (2024--2035)" underscores the importance of fostering students' healthy growth and holistic development, advocating for the widespread integration of mental health education and the creation of tailored service mechanisms across various educational stages. As internet technology continues to advance rapidly and permeate every aspect of modern life, online platforms have become integral to the academic, social, and personal lives of university students. This digital transformation has profoundly reshaped the psychological environment in which students develop, influencing their emotional experiences, cognitive processes, and behavioral decisions. These influences stem not only from the realities of campus life but also from the dynamics of online information dissemination, virtual interactions, and the evolving norms of digital behavior. Consequently, the integration of cybersecurity education into university mental health programs emerges as a critical strategy to address these challenges. By equipping students with the knowledge and skills to navigate the digital landscape responsibly, universities can enhance their mental resilience and adaptability. This paper explores the value of such integration, identifies practical challenges, and proposes implementation strategies aimed at optimizing mental health

Received: 03 February 2026

Revised: 11 March 2026

Accepted: 25 March 2026

Published: 31 March 2026



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

education systems [1, 2]. The ultimate goal is to empower students to thrive in an increasingly interconnected and digitalized world while safeguarding their psychological well-being.

2. The Value of Integrating Cybersecurity Education into University Mental Health Education

2.1. Addressing Cybersecurity Challenges and Enhancing College Students' Psychological Resilience

As the internet becomes increasingly intertwined with college students' academic pursuits, daily routines, and social interactions, its influence on their psychological well-being has become more pronounced. Challenges such as cyberbullying, the spread of misinformation, and online fraud not only result in financial losses and violations of personal rights but also frequently provoke adverse emotional responses, including anxiety, panic, and anger. These emotional disturbances can have long-term implications for students' mental health [1]. Integrating cybersecurity education into university mental health programs equips students with the tools to recognize and mitigate common digital risks. By learning to identify fraudulent schemes, such as impersonation scams, fake lottery notifications, or deceptive transfer requests, students develop heightened vigilance and critical thinking skills, reducing the likelihood of falling victim to such tactics. For example, understanding the psychological manipulation often employed in these scams enables students to respond more rationally and avoid impulsive decisions driven by trust or emotional reactions. Furthermore, cybersecurity education fosters the ability to interpret online interactions and conflicts more effectively. This includes strategies for addressing cyberattacks, verbal harassment, or information overload in a manner that safeguards their rights and prevents the escalation of negative emotions. By teaching students how to navigate these challenges, universities can help them build resilience and maintain emotional stability in the face of digital adversities. Ultimately, cybersecurity education not only enhances safety awareness but also serves as a foundational component for strengthening the psychological resilience of college students, enabling them to thrive in an increasingly digital world.

2.2. Standardize Online Interaction Behaviors and Foster a Healthy Digital Mindset among College Students

Cyberspace is defined by its openness, immediacy, and interactivity, which significantly influence the behaviors and perceptions of college students. As active participants in the digital realm, students often act as information recipients, content creators, and contributors to online discussions. This multifaceted role exposes them to risks such as one-sided information, emotionally charged statements, and inappropriate online behaviors, potentially leading to extreme viewpoints or psychological distress. To address these challenges, integrating cybersecurity education into university mental health programs is essential. Such education equips students with fundamental skills for verifying information accuracy, understanding the limitations of algorithmic recommendations, and recognizing the ethical boundaries of online discourse. Additionally, it fosters awareness of the distinctions between virtual and real-world relationships, encouraging students to maintain appropriate social boundaries and resolve digital conflicts with rationality and maturity. By emphasizing accountability for online actions, students are guided to protect their rights while respecting others' privacy and freedom of expression. This approach cultivates a structured and respectful digital environment, enabling students to navigate the online world with greater composure and resilience [3]. As a result, they are better prepared to manage negative events without succumbing to panic or self-doubt, ultimately enhancing their psychological well-being and fostering a balanced digital mindset.

2.3. Enrich the Content of Psychological Education and Improve the Mental Health Education System in Higher Education Institutions

Currently, college students' learning, social interactions, and self-expression are deeply intertwined with cyberspace, where numerous psychological challenges are often amplified. Issues such as cyberbullying, excessive exposure to information, internet addiction, breaches of privacy, and identity inconsistencies in virtual environments can profoundly affect students' emotional stability, self-esteem, and interpersonal relationships in the real world. Addressing these challenges requires integrating cybersecurity education into university mental health programs, aligning psychological education content more closely with students' actual life experiences. Unlike general mental health education, cybersecurity education emphasizes critical skills such as identifying risks, evaluating information, setting behavioral boundaries, and practicing self-protection. This approach equips students with the tools to monitor their psychological well-being while understanding the influence of the digital environment on their emotions, cognition, and behavior. By fostering these competencies, students can develop rational judgment and maintain balanced engagement in the increasingly complex online landscape [4, 5]. Cybersecurity education is not merely an additional component of mental health education but a foundational element that strengthens the overall framework of mental health support in higher education institutions. Its integration enhances the relevance of mental health programs, enabling universities to address the evolving needs of students in the digital age more effectively. Furthermore, this approach promotes a proactive stance in mental health education, preparing students to navigate the challenges of the digital era with resilience and informed decision-making, ultimately contributing to their holistic development and well-being [6, 7].

3. The Practical Challenges of Integrating Cybersecurity Education into University Mental Health Education

3.1. The Educational Positioning Requires Clarification, and There Is Insufficient Integration between Cybersecurity Education and Psychological Development Education.

Currently, universities face significant challenges in clarifying the educational positioning required to integrate cybersecurity education with mental health education effectively. Administrators and educators often treat these two domains as distinct, with cybersecurity education focusing on technical safeguards and behavioral norms, while mental health education emphasizes emotional guidance, stress management, and interpersonal skills. This separation results in fragmented approaches to curriculum design, activity planning, and resource allocation, which ultimately hinders the seamless integration of these critical areas. From an instructional perspective, cybersecurity educators tend to prioritize technical topics such as password management, phishing detection, and virus prevention, often relegating these issues to IT departments rather than addressing their psychological implications. On the other hand, mental health instructors typically focus on traditional concerns like academic stress, emotional regulation, and social interactions, frequently neglecting emerging challenges such as internet addiction, virtual identity conflicts, and online social anxiety [8]. This dichotomy creates a gap in students' ability to apply theoretical knowledge to practical scenarios. For instance, students may know how to report cyberattacks or block online threats but struggle to manage the anxiety or social withdrawal that may accompany such incidents. Similarly, while they might understand psychological coping strategies, they often lack awareness of critical online privacy measures and the ability to discern reliable information in digital spaces. These ambiguities in educational frameworks disrupt both administrative and instructional planning, undermining the development of students' comprehensive skills to navigate the complexities of real-world digital environments. Addressing these challenges requires a more integrated approach that bridges the technical and psychological aspects of education, ensuring that students are equipped to handle both the technical and emotional dimensions of cybersecurity in their daily lives.

3.2. The Collaborative Mechanism Remains Inadequate, with Poor Alignment between Institutional Design and Practical Implementation.

Integrating cybersecurity education into university mental health programs necessitates a robust and well-coordinated institutional framework. However, in practice, these two domains often function independently, managed by separate administrative departments with distinct planning, resource allocation, and implementation processes. This separation results in fragmented efforts and a lack of cohesive strategies. Academic departments frequently design curricula, course outlines, and instructional content for cybersecurity education and mental health education as isolated components, which hinders the effective integration of resources and activities. Similarly, student affairs departments often fail to provide comprehensive guidance on merging these aspects into extracurricular initiatives or daily educational practices, further exacerbating the disconnect. At the departmental level, some faculty members and counselors have acknowledged the psychological impact of issues such as cyberbullying, online fraud, and information overload on students. They have made efforts to incorporate relevant case studies into class meetings, ideological education courses, or specialized teaching sessions. However, these initiatives are typically driven by individual experience rather than being part of a systematic or sustained approach. Limited resources, divided faculty attention, and evaluation mechanisms that do not align with integration goals further undermine these grassroots efforts. Consequently, these challenges prevent consistent and effective outcomes. The absence of a stable collaborative mechanism between institutional design and frontline implementation remains a critical barrier. Addressing this issue requires a comprehensive strategy that aligns administrative structures, resource allocation, and evaluation systems to foster a more integrated and effective approach to combining cybersecurity education with mental health support.

3.3. Faculty Support Is Relatively Insufficient, and the Content Formats Do Not Adequately Meet Student Needs.

Integrating cybersecurity education into college mental health education requires a multifaceted approach that combines qualified teaching staff with content and delivery methods tailored to students' actual needs. Cybersecurity educators often excel in technical aspects such as protection mechanisms and risk identification but may lack a nuanced understanding of the psychological and emotional factors influencing online behaviors. On the other hand, mental health educators bring expertise in psychological counseling but may struggle to keep pace with the rapidly evolving challenges of the digital age, including online fraud, information cocoons, and cyberbullying. This disconnect highlights the need for interdisciplinary collaboration to bridge these gaps effectively. Existing educational content frequently emphasizes risk warnings and rule-based frameworks, which, while important, fail to deeply engage with the lived online experiences of college students. Traditional delivery methods, such as lectures, reports, and informational brochures, often position students as passive recipients of information, limiting opportunities for active engagement through contextual discussions, case studies, and interactive learning experiences. This lack of dynamic and relatable content delivery is particularly problematic when addressing specific issues like online social anxiety, privacy breaches, public opinion conflicts, and addiction to short-video platforms. These challenges require educational formats that not only inform but also empower students to develop critical thinking, active judgment, and self-regulation skills [9, 10]. The current reliance on monolithic educational approaches diminishes the resonance and effectiveness of these programs, underscoring the urgent need for innovative and student-centered strategies. By addressing these deficiencies in content provision and delivery formats, institutions can better equip students to navigate the complex interplay between cybersecurity and mental health in their daily lives.

4. Practical Approaches for Integrating Cybersecurity Education into University Mental Health Education

4.1. Clarify the Educational Positioning and Promote the Transition of Both Approaches from Fragmented Parallelism to Organic Integration

To effectively integrate cybersecurity education into university mental health programs, it is crucial to first redefine educational perspectives and establish the intrinsic connection between these two domains. Universities must acknowledge that cybersecurity concerns are not limited to technical safeguards or behavioral norms; they are deeply intertwined with students' cognitive processes, emotional resilience, interpersonal relationships, and self-perception. Consequently, institutions should reposition cybersecurity education as a fundamental element within the broader framework of mental health education, emphasizing its importance in risk assessment, behavioral guidance, psychological adaptation, and self-protection strategies. Implementation should focus on achieving conceptual alignment and coherence in educational goals. Cybersecurity education should be embedded into annual mental health initiatives, transitioning from isolated campaigns to a consistent and integral component of psychological development programs [11]. Furthermore, mental health courses and daily educational activities should incorporate content tailored to online contexts, addressing critical topics such as countering online misinformation, managing emotional responses, establishing social boundaries, enhancing communication skills, safeguarding privacy, and developing self-defense mechanisms. These efforts aim to help students comprehend the profound relationship between their digital behaviors and overall mental well-being. By harmonizing educational objectives and coordinating content delivery, cybersecurity education and mental health education can evolve from fragmented, parallel disciplines into a seamlessly integrated system that supports holistic student development. This approach not only enhances the effectiveness of both educational areas but also equips students with the necessary tools to navigate the complexities of the digital age while maintaining their mental health and emotional stability.

4.2. Improve the Operational Mechanisms to Ensure Effective Integration between Top-Level Design and Grassroots Implementation

To effectively integrate cybersecurity education into university mental health programs, it is essential to establish a robust operational mechanism that ensures seamless coordination between institutional oversight, interdepartmental collaboration, and departmental implementation. Universities should embed these elements into their overarching plans for mental health education and student safety initiatives, clearly defining objectives, content frameworks, implementation steps, and evaluation criteria. This approach will provide systematic support and ensure sustained execution. Key components such as digital literacy, risk identification skills, and psychological adaptation to online environments should be incorporated into student competency assessments or mental health evaluations. These measures will enhance the regulatory framework and provide a guiding influence for integrated education. Interdepartmental coordination should involve a collaborative mechanism that includes academic affairs offices, student affairs departments, cyberspace administration authorities, mental health centers, and academic departments. Academic affairs offices should focus on curriculum integration and credit recognition, while student affairs departments manage daily educational activities and gather feedback. Cyberspace authorities can offer technical support, issue risk alerts, and conduct online sentiment analysis. Mental health centers should prioritize psychological needs assessments, crisis identification, and interventions, while academic departments implement measures tailored to specific disciplinary characteristics and student needs. Joint meetings, thematic analyses, and information sharing can help minimize fragmented efforts and resource dispersion among departments [12, 13]. At the departmental level, integrated education should be incorporated into class discussions, specialized courses, club activities, and counseling sessions, aligning with students' academic profiles and practical needs. Counselors can provide guidance on online interaction boundaries, privacy protection, and managing online discourse, while departments may organize case studies or thematic workshops to deepen understanding. This comprehensive approach will transition integrated education

from sporadic experimentation to sustained practice, ensuring that students are equipped with the necessary skills to navigate the complexities of the digital world while maintaining their mental well-being.

4.3. Strengthen Teacher Empowerment to Enhance the Synergy between Cybersecurity and Psychological Education

Teachers play a pivotal role in the effective integration of cybersecurity education with mental health education, as their professional expertise significantly influences the quality and success of such interdisciplinary approaches. Universities should prioritize the establishment of comprehensive teacher development mechanisms that align with the core competencies required for addressing the intersection of digital environments and psychological well-being. These competencies include understanding cyberspace, identifying potential risks, providing appropriate guidance, and implementing timely interventions. By equipping educators with these skills, institutions can ensure that teachers are well-prepared to address the multifaceted challenges posed by the digital age. Practical strategies to achieve this include fostering collaborative lesson planning sessions, conducting in-depth case studies, organizing specialized training programs, and implementing practical supervision frameworks. These initiatives encourage knowledge sharing and skill enhancement among faculty members. For example, mental health instructors could participate in cybersecurity case analyses to gain insights into real-world digital threats, while cybersecurity educators could undergo mental health training to develop essential communication skills and techniques for identifying and addressing psychological crises [14]. Counselors, as primary points of contact with students, should take on dual roles that involve monitoring online behaviors and providing psychological support through class management, themed discussions, and one-on-one consultations. To further incentivize active participation, universities should integrate teachers' contributions to this integrated educational approach into their professional development records, performance evaluations, and overall assessments of educational effectiveness. By fostering a culture of continuous learning and collaboration, institutions can build a robust, multidisciplinary support system. This system will ensure the seamless integration of cybersecurity education into university mental health programs, ultimately promoting a holistic approach to student well-being in the digital era.

4.4. Innovate Content and Approaches to Build a Comprehensive Integrated Education System

The integration of cybersecurity education into university mental health programs necessitates a comprehensive restructuring of both educational content and implementation strategies, ensuring alignment with the real-world contexts of students' online activities. Universities must systematically address prevalent challenges and risks associated with digital usage by embedding key elements such as information discernment, privacy protection, and self-protection awareness into their curricula. This approach should establish a progressive educational framework encompassing cognitive guidance, risk identification, behavioral regulation, and psychological support. To enhance learning outcomes, educational methods should prioritize experiential learning and active student participation. Faculty members can utilize real-world scenarios, including social pressures online, dependence on virtual relationships, and excessive information exposure, to facilitate critical analysis of the interplay between online behaviors and psychological states. Through scenario-based analysis, group discussions, peer collaboration, and reflective documentation, students can develop essential skills to assess risks, manage emotions, maintain boundaries, and seek support, transforming the educational process from passive reception to active engagement. Furthermore, universities should implement tiered education tailored to different developmental stages. Orientation programs for freshmen should emphasize internet etiquette, personal data protection, and adaptability training. During subsequent academic years, the focus should shift to online communication skills, information filtering, emotional management, and addiction prevention. For graduating students, the curriculum should prioritize online image management, employment information literacy, and social adaptation skills. By

adopting stage-specific designs, context-driven approaches, and continuous implementation, these initiatives can be seamlessly integrated into university mental health systems [13]. Such integration significantly enhances the support provided for students' holistic development, equipping them with the tools to navigate the complexities of the digital age while fostering resilience and adaptability in their mental health and overall well-being.

5. Conclusion

In summary, integrating cybersecurity education into university mental health programs represents a crucial initiative for institutions to adapt to evolving digital learning environments. This integration not only addresses the increasing prevalence of cyber threats but also acknowledges the psychological toll that such threats can impose on students. Universities must adopt a multifaceted approach, coordinating efforts across educational philosophies, operational frameworks, faculty development, and instructional methodologies. By fostering a seamless synergy between cybersecurity education and mental health support, institutions can empower students to develop robust skills in identifying and mitigating cyber risks while simultaneously enhancing their capacity to manage psychological stress. Furthermore, this initiative promotes holistic development by equipping students with the resilience and adaptability needed to thrive in both digital and real-world contexts. Future research should explore innovative pedagogical strategies, assess the long-term impacts of such programs, and identify scalable models for broader implementation across diverse educational settings.

Funding: Research Project of the Party Building Research Professional Committee of Private Universities of the Hainan Provincial Party Building Research Association in 2026: "Research on the Practical Path of Integrating the" One stop "Student Community of Private Universities into the Education of the Awareness of the Chinese National Community under the Guidance of Party Building" (Project Number: HNMD2026YB-15)

References

1. M. Gallagher and J. Lamb, "Open education in closed-loop systems: Enabling closures and open loops," *Distance Education*, vol. 44, no. 4, pp. 620-636, 2023.
2. J. E. Volkman, B. M. Wolf, C. Morse, E. Browning, A. High, H. P. Lacey, ... and W. Samter, "Exploring college-aged student anxiety: Aggravating factors and coping strategies," 2024.
3. X. Zhang, "Problems and countermeasures of college students' mental health education," *Journal of Healthcare Engineering*, vol. 2022, no. 1, p. 6430855, 2022.
4. W. Yuan, "Exploring the path of modern transformation of mental health education for university students," *Applied & Educational Psychology*, vol. 4, no. 9, pp. 71-75, 2023.
5. S. Yang, L. Lin, and X. Zhang, "Adjustment method of college students' mental health based on data analysis under the background of positive psychology," *Frontiers in Psychology*, vol. 13, p. 921621, 2022.
6. J. Crabb, C. Hundhausen, and A. Gebremedhin, "A critical review of cybersecurity education in the United States," in **Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1**, Mar. 2024, pp. 241-247.
7. W. J. Triplett, "Addressing cybersecurity challenges in education," *International Journal of STEM Education for Sustainability*, vol. 3, no. 1, pp. 47-67, 2023.
8. J. Ricci, F. Breitingger, and I. Baggili, "Survey results on adults and cybersecurity education," *Education and Information Technologies*, vol. 24, no. 1, pp. 231-249, 2019.
9. E. S. Koc, "Fostering mental-wellbeing and health behavior through online learning measures and cyber resilience," *American Journal of Health Behavior*, vol. 48, no. 4, pp. 1039-1048, 2024.
10. A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches," *Symmetry*, vol. 15, no. 12, p. 2175, 2023.
11. B. Inkster, C. Knibbs, and M. Bada, "Cybersecurity: A critical priority for digital mental health," *Frontiers in Digital Health*, vol. 5, p. 1242264, 2023.
12. N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378-382, 2020.
13. M. Mukherjee, N. T. Le, Y. W. Chow, and W. Susilo, "Strategic approaches to cybersecurity learning: A study of educational models and outcomes," *Information*, vol. 15, no. 2, p. 117, 2024.

14. I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's'," *Heliyon*, vol. 5, no. 12, 2019.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of Publisher and/or the editor(s). Publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.