ISSN: 2182-2069 / E-ISSN: 2182-2077

Psychological Profiling for Enhancing Cybersecurity Training Effectiveness in Educational Institutions

Jamila Djumabaeva[1*], Shakhnoza Akramova[2], Gavhar Nurkulova[3], Nodira Xatamova[4], Yulduzxon Abulkasimova[5], Zoir Botirov[6], Zilola Yunusova[7], and Asal Kasimova[8]

[1*]Professor, National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan. djumabaevajamila@gmail.com, https://orcid.org/0000-0003-0117-1648

[2]University of Public Safety of the Republic of Uzbekistan, Tashkent, Uzbekistan. xabibasevinch@mail.ru, https://orcid.org/0009-0001-0675-0000

[3]Department of Psychology, Termez State University, Uzbekistan. nurqulovagavhar@gmail.com, https://orcid.org/0009-0008-6928-8272

[4]Department of Foreign Languages, Tashkent State University of Law, Uzbekistan. nodira.xatamova@tsul.uz, https://orcid.org/0000-0002-2494-3877

[5]Teacher, Foreign Languages Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmiy, Uzbekistan. yulduzxonabulkasimova@gmail.com, https://orcid.org/0000-0002-6309-6551

[6]Lecturer, Department of Psychology, Termez State University, Termez, Uzbekistan. botirovzoirbek3@gmail.com, zbotirov@tersu.uz, https://orcid.org/0009-0006-8632-3338

[7]Senior Teacher, Journalism and Mass Communications University of Uzbekistan, Uzbekistan. zilola27.78@gmail.com, https://orcid.org/0009-0002-4400-142X

[8]Associate Professor, International Public Law, Tashkent State Transport University, Tashkent, Uzbekistan. asal.kasimova78@gmail.com, https://orcid.org/0009-0001-3440-0251

Received: March 10, 2025; Revised: April 18, 2025; Accepted: May 15, 2025; Published: May 30, 2025

Abstract

It is well accepted that human factors impact almost every aspect of cybersecurity. Users often tend to act by clicking links in phishing emails without considering the possible consequences. Cyber attackers are influenced by psychological factors such as motivation, social identity, and group dynamics. Moreover, various psychological factors like cognitive load, mental health, trust, and interpersonal relationships also facilitate insider threats, intentionally or unintentionally. Incorporating psychological approaches to cybersecurity education can empower practitioners to address myriad security challenges more effectively. Creating these enhancements is problematic because applying psychology involves many theories and methods, most of which would not be useful in cybersecurity. It is important to sift through psychological literature for concepts that can be applied to cybersecurity. In addition, differences in approaches to teaching psychology compared to cybersecurity and the predominant psychological characteristics of students attracted to both subjects also exist. Addressing these differences is important for motivating and engaging cybersecurity learners. This paper addresses these concerns and provides reflections on the results

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 953-963.
DOI: *10.58346/JISIS.2025.I2.063*

*Corresponding author: Professor, National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan.

of interdisciplinary collaboration in teaching psychology to students, professionals, and industry clients in cybersecurity.

Keywords: Psychological, Threats, Students, Interdisciplinary Collaboration, Characteristics, and Professionals.

1 Introduction

There has been minimal practical research studying the cognitive skills, communication, and collaboration underpinning performance in cybersecurity occupations (Bandura, 2003) (Dawson & Thomson, 2018). This paper outlines how psychology has been integrated into cybersecurity curricula to assist professionals in understanding human behavior related to technical work (Hoa & Voznak, 2025). Cybersecurity incidents should be understood as behavioral events driven by distinct psychological factors (Mokoena & Nilsson, 2023). Cyber attackers often exploit these psychological mechanisms, reinforcing the idea that humans are generally the weakest link in cybersecurity, primarily through social engineering tactics such as phishing (Kearney & Kruger, 2016). Despite the clear importance of the human factor in complex systems, psychological content is largely absent in cybersecurity education and training programs (Rajan & Srinivasan, 2025; Alsharifi, 2023). This absence is surprising given the extensive psychological knowledge and research related to cybersecurity, including motivation, behavior prediction, policymaking and human-policy interface, usability engineering, behavior change, and organizational culture change (Darley, 1992). These topics are regularly covered in psychology courses and professional training on behavior change in business and industry, demonstrating that behavioral pedagogy can improve cybersecurity education (Taylor, 2008).

The integration of psychology within cybersecurity is likely limited due to fundamental differences between the disciplines. Psychology spans a wide range of areas, some of which are quantitatively and technologically driven, such as neuropsychology. Cybersecurity training often lacks the time to provide a comprehensive overview of psychological methods, nor would this be practical. Furthermore, psychology and cybersecurity differ in their underlying philosophical assumptions. Psychology tends to borrow perspectives from social sciences, especially social constructionism, which views human experiences as the product of subjective social interpretations. In contrast, technology and engineering disciplines take a constructionist approach, assuming that objective truths determine the existence of phenomena (Lahon & Chimpi, 2024). Addressing these epistemological and ontological considerations is critical for teaching psychology effectively to cybersecurity students (Taylor, 2008).

This paper focuses on two major problems encountered in the interdisciplinary approach of teaching psychology in cybersecurity training programs: first, identifying the psychological concepts and issues most relevant to cybersecurity students; second, developing methods to bridge the ontological and epistemological divides between psychology and cybersecurity education for more effective interdisciplinary learning (Singh & Kumar, 2024).

The paper's structure is as follows: Section 2 reviews the integration of psychological theories in cybersecurity education. Section 3 examines the application of psychology-based training tools in workplace settings. Section 4 discusses key findings and practical implications. Finally, Section 5 concludes with recommendations for future interdisciplinary research and practice.

2 Identifying Relevant Areas of Psychology

Cybersecurity issues are complex and multifactorial. Many psychological domains could be relevant, but this subsection examines psychology through the perspectives of cyber adversaries and victims to narrow down applicable areas.

2.1 The Adversaries

Cyber attackers commonly use social engineering tactics such as phishing. While early phishing scams used obvious errors and blatant manipulation, current phishing attacks are deceptively sophisticated and successfully trick up to 45% of targeted users. Phishing exploits heuristics—decision-making shortcuts simplifying complex social and environmental challenges. For example, phishing emails may misuse company logos to authenticate their legitimacy falsely. Protection Motivation Theory explains how fear appeals, such as fake bank account alerts, can push users to take overly risky actions (Rogers, 1975) (Gibbs, 2003). However, not all techniques promoted by social engineers stand up to scientific scrutiny; for instance, neuro-linguistic programming is often touted by attackers but dismissed as pseudoscience by psychologists (Hadnagy, 2011). This highlights the importance of grounded psychological evidence within cybersecurity policy frameworks (Bursztein et al., 2014).

Understanding adversaries' psychological behaviors aids threat recognition. Analysis of adversaries' conversations on chat forums reveals cognitive dissonance, with many rationalizing their harmful actions using guilt reduction strategies such as euphemistic language, blame shifting, minimizing impact, and victim dehumanization (Witkowski, 2010; Rogers, 2010). Recognizing these defense behaviors helps cybersecurity professionals better assess threats and distinguish credible risks from noise (Maurushat, 2019; Wallach et al., 1962).

Logic and social identity are also key motivators for adversarial actions. Various typologies categorize hackers by motives such as prestige, recreation, revenge, profit, or ideology (Seebruck, 2015). Such understanding enables cybersecurity students to anticipate behaviors and take proactive measures. For instance, ideological hacktivists launching distributed denial of service (DDoS) attacks differ fundamentally from financially motivated hackers (Maurushat et al., 2019). Group dynamics also affect adversarial behavior; social psychology research shows group membership can alter perception and judgment, leading to riskier decisions than when acting alone. The category differentiation model further explains how public identification of adversary groups strengthens group bonds, potentially increasing exploit attempts (Schneier, 2008). These psychological insights improve assessments of adversarial actions and cybersecurity problem resolution (Steptoe & Wardle, 2001).

2.2 The Targets

Phishing and social engineering rely on specific target behaviors or inactions. Understanding demographic and individual differences helps explain which populations are more vulnerable. Attackers do not always target the most unsuspecting victims (Iuga et al., 2016). Individuals with cognitive biases may disregard warnings, believing breach impact mitigation outweighs control, while users may grant social network access without scrutiny (O'Connell & Kirwan, 2014). Organizations often fail to implement additional security after breaches, falsely assuming future attacks are predictable, illustrating the privacy paradox (Utz & Kramer, 2009; Rifon et al., 2005). Table 1 illustrates the implications of psychological theory for cybersecurity education along with its relevance to cybersecurity and its educational applications (Banerjee & Kapoor, 2024).

Table 1: Implications of Psychological Theory for Cybersecurity Education

Psychological Theory	Relevance to Cybersecurity	Educational Use
Protection Motivation Theory	Explains how fear-based appeals influence risk-related behaviors	Design warnings that appropriately motivate action without causing panic
Planned Behavior Theory	Highlights how intention is shaped by attitudes, norms, and perceived control	Educate students on influencing user behavior through positive norm reinforcement.
Social Identity Theory	Group membership influences individual risk-taking and decision-making	Helps explain insider threats and group-driven noncompliance
Dual-process Theory (Kahneman)	Fast (impulsive) vs. slow (analytical) thinking governs responses to threats.	Develop training to encourage slower, more cautious user responses.

Other cognitive biases linked to cybersecurity include overestimating rare risks while underestimating common ones, misjudging personal control over risks, feeling less vulnerable than peers, and exaggerating media-publicized threats. These biases serve evolutionary purposes; heuristics allow rapid decision-making amidst information overload, a necessary adaptation despite frustrating cybersecurity experts advocating caution (Sheng et al, 2010; Kahneman, 2011). Exploiters incite fear and urgency to manipulate these tendencies, while psychologists recommend designing systems around inherent cognitive biases to improve user decisions. Table 2 depicts the psychological factors influencing target vulnerability in cybersecurity.

Table 2: Psychological Factors Influencing Target Vulnerability in Cybersecurity

Psychological Factor	Description	Implication for Cybersecurity
Cognitive Biases	Biases like overconfidence, optimism bias, and risk misperception	Users may ignore warnings, underestimate threats, or over-trust communications
Heuristics and Decision-making	Mental shortcuts used to manage information overload	Attackers exploit these for fast, emotional reactions (e.g., urgency in phishing)
Privacy Paradox	Discrepancy between privacy concerns and actual behavior	Users share data or skip security steps despite privacy awareness
Perceived Social Norms	Belief about what others expect or approve of	Users may neglect updates to avoid disapproval or workflow interruption
Group Dynamics	Peer influence and social identity in the workplace	Can encourage noncompliance or enable insider threats
Psychosocial Stressors	Workplace stress and interpersonal conflict	Increases likelihood of unintentional errors or malicious insider behavior

Adversarial actors often operate within social groups, influencing cybersecurity behaviors. Informal group dynamics can facilitate or obstruct security compliance. For example, planned behavior theory suggests actions like software updates are influenced by expected social approval (Venkatesh et al, 2003). Users may avoid updates, fearing supervisory disapproval due to downtime. Social relationships also contribute to insider threats, with psychosocial workplace factors such as interpersonal conflict and stress increasing risk (Band et al., 2013). Incorporating psychological pedagogy helps cybersecurity students recognize and assess such psychosocial elements effectively.

3 Pedagogical Approaches

Integrating psychology into cybersecurity education requires attention to both content and instructional methods. Cybersecurity students often view psychology narrowly as mental pathology or hobbies, though psychology extends far beyond into rigorous scientific study of behavior and cognition. Psychology is a Bachelor of Science discipline in many countries, reflecting its scientific basis (Taylor, 2008). Differences in ontology and epistemology between psychology and computing shape student receptiveness to educational approaches. This informed the authors' teaching of psychological cybersecurity principles to various student and professional cohorts.

3.1 Understanding Student Motivations and Expectations

Cybersecurity students vary widely, from recent school leavers to experienced professionals. Research indicates computing students prioritize problem-solving and critical thinking for employability, whereas psychology students seek understanding of behavior, social dynamics, and self-development. Psychology students are more interested in sociocultural relations, while computing students focus on technical systems. Recognizing these motivational and experiential differences is crucial in designing effective cybersecurity education (Radford & Holdstock, 1995). Table 3 illustrates the expectations and motivations of students with regard to cybersecurity psychology education.

Table 3: Understanding Student Motivations and Expectations in Cybersecurity Psychology Education

Student Group	Primary Motivations	Common Expectations	Pedagogical Implications
Undergraduate Students	Career readiness, skills development, and curiosity	Practical examples, simplified theory	Use engaging real-life case studies and simulations
Postgraduate Students	In-depth knowledge, research opportunities, and specialization	Advanced theory, interdisciplinary integration	Offer project-based learning and comparative frameworks
Industry Professionals	Upskilling, compliance knowledge, and incident response capability	Real-world application, time-efficient content	Focus on practical relevance, modular training, and time flexibility
Psychology Background	Human behavior, mental processes, and social influence	Link to known theories, real-life psychological mechanisms	Bridge concepts to technical language and cybersecurity contexts
Computer Science Background	Technical solutions, coding, and security architecture	Concrete answers, algorithmic thinking	Introduce psychological theory through structured and objective models
Mature Learners	Career switch, policy influence, strategic leadership roles	Respect for experience, applicable knowledge	Blend theory with policy and ethical discussions

Younger undergraduates across backgrounds often lack confidence in discussing ethical, moral, and philosophical issues, suggesting that maturity should be factored into pedagogy. Additionally, students accustomed to computing's binary problem-solving culture may struggle with psychology's plurality of theories, often asking, "Which psychological theory is correct?" reflecting surprise or frustration at the lack of universal acceptance.

3.2 Perspective Shifting

Cybersecurity students focus on attack mechanics and consequences rather than adversaries' motivations. Encouraging multiple perspectives deepens understanding. For example, students analyze high-risk groups, tailor advice, and devise countermeasures considering attacker and target behavior, engaging with complex psychological processes (Johnston et al., 2015).

Psychology also supports digital investigation and forensics, where behavioral profiling aids in constructing password dictionaries (Linn et al., 2011). This integration enhances cyber forensic effectiveness and highlights psychology's role in managing the uncertainty inherent in cybercrime analysis (Schmidt & Arnett, 2005).

Cybersecurity responses often involve technical controls like new authentication or stricter policies, which may increase inefficiency and user burden without addressing root causes. Psychological design principles emphasize user-centered protective systems that avoid aggravating users. The concept of "desirable difficulties," interruptions prompting heightened user attention at critical moments, guides students to develop frameworks aligned with human behavior, improving cyberspace usability (Bjork & Bjork, 2011).

4 Teaching Psychology in the Workplace

The teaching outcomes in psychology and cybersecurity are now forming the basis for designing commercial tools intended to enhance organizational practices for improving cybersecurity. However, there are important differences in the context of the academic environment in colleges and universities and the professional world. While cybersecurity students might not appreciate the role of psychology, it is safe to say that they would probably have some interest in cybersecurity. The most significant hurdle within academic bounds is the need to make a convincing case as to why psychology, within the frameworks of the disciplines taught, is important relative to cybersecurity issues. On the contrary, in companies, employees do not care about cybersecurity. Even where interest exists, the time and budgetary confines of the workplace mean that cybersecurity education has to be more strategic and delivered in less time as shown in Figure 1.

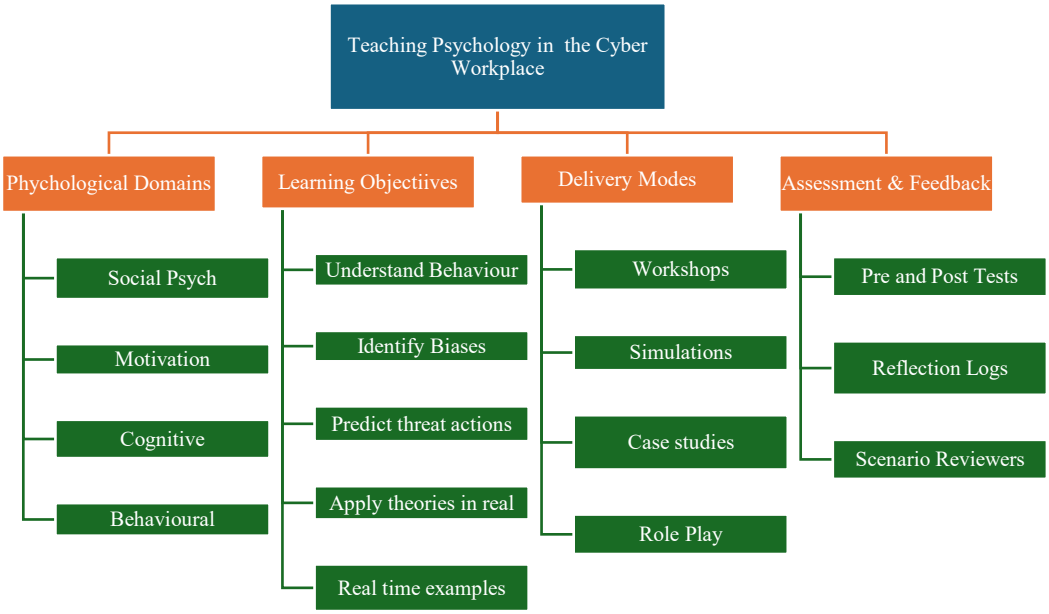

Figure 1. Teaching Psychology in the Workplace

In the UK, we have collaborated positively with LiMETOOLS, a niche publisher of behavioral change learning tools in high-risk commercial areas such as cybersecurity. Using social cognitive learning theory, employees consider how their actions might enable cyberattacks through perspective-taking exercises akin to those used in student teaching. Learners role-play interactive dramas in critical cybersecurity situations and take comprehension tests afterwards. One tool, tailored for graduates who are heavy users of social networking platforms, offers a detailed treatment of social engineering techniques that are widely misused. This tool emulates the actions of a fictitious hacker and motivates learners to develop personal strategies that the system will track algorithmically. Another tool, aimed at graduate recruiters, teaches them to educate the new employees by auditing their cyber vulnerabilities through numerous industry-relevant domains.

In Australia, a common strategy includes HATCH Training (Hacking and Tricking Capricious Humans), which teaches employees how to identify and respond to various methods of cyberattacks through real-time simulation exercises. This method helps address phishing, ransomware, physical security breaches, and spear phishing attacks. Furthermore, large companies now routinely use simulation-based training incorporating live-action role-playing elements, providing participants with realistic scenarios and solutions. These role-played portions evaluate how faux targets would respond to psychological exploitations, thus significantly improving the employees' cybersecurity awareness. In addition, some better-funded companies exploit behavioral psychology to deal with entrenched cultural cognitive vulnerabilities, biases, and overconfidence regarding defences designed to mitigate risks. This permits customized, bespoke filters tailored to the weaknesses of the person applying.

From these approaches, key insights distil into two main points needing integration of psychological and technological aspects in workplace-dedicated cybersecurity training: i) Incorporating video or dramatized portrayals into lessons as part of the curriculum leads to higher engagement with younger learners. ii) Intellectual challenges accompanied by well-structured, psychologically sound games and positive feedback elevate participation, change behavior, and increase retention of information. iii) psychological research indicates that having control over the pace of learning and the tools used to learn enhances autonomy, which helps in behavior change. iv) Participants attempting to circumvent overly lengthy activities or "backsolving" tend to work around the system. This suggests a balanced combination of interactive sessions, quizzes, and videos yields the best results. v) Many participants claimed that instead of the anticipated help, the videos made them more anxious by not showing them how to help. This directly relates to Protection Motivation Theory, whereby too much fear becomes too paralyzing when there is no effective action. To alleviate this discomfort, the training offers modules that enable participants to develop positive, actionable plans to replace gaps that the negative scenarios present. V) Tracking systems through Learning Management Systems are beneficial because they allow learners to view their progress and comparative scores. This visual feedback of ongoing progress may encourage sustained interaction. Table 4 depicts the efficiency of various training approaches in workplace cybersecurity education and Figure 2 depicts the training methods in workplace cybersecurity education

Table 4. Effectiveness of Different Training Methods in Workplace Cybersecurity Education

Training Method	Engagement Level (%)	Behavior Change (%)	Participant Compliance (%)
Multimedia Content (Videos)	85	78	80
Gamified Intellectual Challenges	90	85	88
Autonomy in Training	75	82	76
Balanced Format (Mixed methods)	80	75	83
Fear Appeals (with guidance)	70	60	65
Fear Appeals (without guidance)	40	30	35
Progress Tracking (LMS)	88	80	90

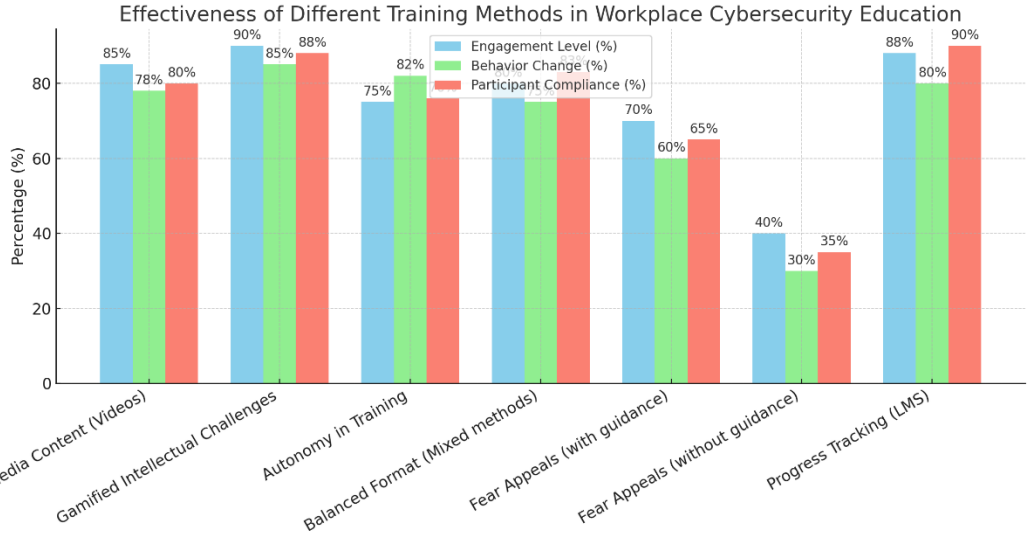

Figure 2: Training Methods in Workplace Cybersecurity Education

5 Conclusions

The paper addressed a firm conviction that psychology can remarkably improve the practice and pedagogy of cybersecurity. To achieve this, we must ascertain what psychological research areas can best serve practical cybersecurity training needs. Equally important is the recognition of the different epistemological and ontological positions held by the students of psychology and students of cybersecurity and the implications these differences have on pedagogy. Interdisciplinary collaboration is essential to adequately equip cybersecurity students and practitioners with the appropriate competencies and insights to meet growing cybersecurity concerns.

References

[1] Alsharifi, A. K. H. (2023). Total quality management strategies and their impact on digital transformation processes in educational institutions. An exploratory, analytical study of a sample of teachers in Iraqi universities. *International Academic Journal of Organizational Behavior and Human Resource Management, 10*(1), 1–16. https://doi.org/10.9756/IAJOBHRM/V10I1/IAJOBHRM1001

[2] Bandura, A. (2003). Social cognitive theory. In R. B. Ewen (Ed.), *An introduction to the theories of personality* (pp. 365–386). Lawrence Erlbaum Associates.
[3] Banerjee, R., & Kapoor, M. (2024). The relationship between education and fertility rates: A comparative study of developing and developed countries. *Progression Journal of Human Demography and Anthropology, 2*(4), 8–14.
[4] Bjork, E. L., & Bjork, R. A. (2011). Making things hard on yourself, but in a good way: Creating desirable difficulties to enhance learning. In *Psychology and the real world: Essays illustrating fundamental contributions to society*. 2, 59–68.
[5] Bursztein, E., et al. (2014). Handcrafted fraud and extortion: Manual account hijacking in the wild. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 347–358). ACM.
[6] Darley, J. M. (1992). Social organization for the production of evil. *Psychological Inquiry, 3*(2), 199–218.
[7] Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9*, 744. https://doi.org/10.3389/fpsyg.2018.00744
[8] Gibbs, J. C. (2003). *Moral development and reality: Beyond the theories of Kohlberg and Hoffman*. SAGE Publications.
[9] Hadnagy, C. (2011). *Social engineering: The act of human hacking*. Wiley Publishing Inc.
[10] Hoa, N. T., & Voznak, M. (2025). Critical review on understanding cyber security threats. *Innovative Reviews in Engineering and Science, 2*(2), 17–24. https://doi.org/10.31838/INES/02.02.03
[11] Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences, 6*(1), 8.
[12] Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.
[13] Kahneman, D. (2011). *Thinking, fast and slow* (1st ed.). Penguin.
[14] Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46–58.
[15] Lahon, S., & Chimpi, K. (2024). Fostering sustainable technological development in SMEs from developing nations within the framework of the digital economy and resource-constrained environments. *Global Perspectives in Management, 2*(4), 15–25.
[16] Linn, M. C., Chang, H. Y., Chiu, J., Zhang, H., & McElhaney, K. (2011). Can desirable difficulties overcome deceptive clarity in scientific visualizations? In A. S. Benjamin (Ed.), *Successful remembering and successful forgetting: A Festschrift in honor of Robert A. Bjork* (pp. 239–262). Taylor & Francis. https://doi.org/10.4324/9780203842539
[17] Maurushat, A. (2019). *Ethical hacking*. University of Ottawa Press.
[18] Maurushat, A., Bello, A., & Bragg, B. (Forthcoming 2019). Artificial intelligence-enabled cyber fraud: A detailed look into payment diversion fraud and ransomware. *Indian Journal of Law and Technology*.
[19] Mokoena, G., & Nilsson, J. (2023). A sophisticated cybersecurity intrusion identification model using deep learning. *International Academic Journal of Science and Engineering, 10*(3), 17–21. https://doi.org/10.71086/IAJSE/V10I3/IAJSE1026
[20] O'Connell, R., & Kirwan, G. (2014). Protection Motivation Theory and online activities. In A. Power & G. Kirwan (Eds.), *Cyberpsychology and new media: A thematic reader*. Psychology Press.
[21] Olson, P. (2012). *We are anonymous*. Back Bay Books.
[22] Radford, J., & Holdstock, L. (1995). Gender differences in higher education aims between computing and psychology students. *Research in Science & Technological Education, 13*(2), 163–176.

[23] Rajan, A., & Srinivasan, K. (2025). Automated incident response systems for cybersecurity. In *Essentials in Cyber Defence*. 1–15. Periodic Series in Multidisciplinary Studies.
[24] Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339–362.
[25] Rogers, M. K. (2010). The psyche of cybercriminals: A psycho-social perspective. In G. Ghosh & E. Turrini (Eds.), *Cybercrimes: A multidisciplinary analysis*.
[26] Schmidt, M. B., & Arnett, K. P. (2005). Spyware: A little knowledge is a wonderful thing. *Communications of the ACM, 48*(8), 67–70.
[27] Schneier, B. (2008). The psychology of security. In *First International Conference on Cryptology in Africa, Lecture Notes in Computer Science*. Casablanca, Morocco.
[28] Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36–45.
[29] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373-382).
[30] Singh, N., & Kumar, A. (2024). Gamification in medical terminology learning: A comparative study of digital education tools. *Global Journal of Medical Terminology Research and Informatics, 2*(1), 4–7.
[31] Steptoe, A., & Wardle, J. (2001). Locus of control and health behaviour revisited: A multivariate analysis of young adults from 18 countries. *British Journal of Psychology, 92*(Pt 4), 659–672.
[32] Taylor, J. (2008). Teaching psychology to computing students. *Psychology Teaching Review, 14*(1), 21–29.
[33] Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2).
[34] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.
[35] Wallach, M. A., Kogan, N., & Bem, D. J. (1962). Group influence on individual risk-taking. *Journal of Abnormal Psychology, 65*(2), 75.
[36] Witkowski, T. (2010). Thirty-five years of research on neuro-linguistic programming. NLP research data base. State of the art or pseudoscientific decoration? *Polish Psychological Bulletin*.

Authors Biography

Jamila Djumabaeva, Professor of English Linguistics at National University of Uzbekistan. Her research focuses on philology, linguistic cognition, and educational psychology. She connects language with behavioral cybersecurity training models. Jamila promotes curriculum reforms for digital resilience in education. She contributes to interdisciplinary teaching with cybersecurity focus. Her work highlights profiling methods for tailored cyber awareness programs.

Shakhnoza Nazirova, PhD in Philological Sciences, Senior Teacher, National University of Uzbekistan. Her research includes VANET-based learning for field linguistics. She supports mobility-based academic apps for contextual language learning. Shakhnoza develops content for location-based teaching modules. Her work promotes safe academic exploration via mobile systems. She leads projects linking transport tech and linguistics education.

Nodira Xatamova, Lecturer, Department of Foreign Languages, TSU of Law. Her expertise is in English for legal purposes and digital learning content. She integrates secure communication into legal English instruction. Nodira's research focuses on language-based awareness for cybersecurity. She also contributes to secure ESP modules in law education. Her work bridges legal terminology and Cyber Behavior Modeling.

Yulduzxon Abulkasimova, Faculty at TUIT, Foreign Languages Department. She focuses on cybersecurity literacy in English language training. Yulduzxon works on integrating digital safety in online communication. Her research includes ESP content aligned with cyber-ethics. She supports multilingual platforms with secure access systems. Her current interest is language-driven awareness for data safety.

Gavhar Nurkulova, Lecturer, Department of Psychology, Termez State University, Uzbekistan. Her academic interests include cognitive psychology, learning behavior, and digital adaptability. She explores psychological factors influencing cybersecurity awareness in academic environments. Gavhar focuses on profiling techniques to improve the effectiveness of digital safety training. She supports interdisciplinary research integrating psychology with educational technologies. Her work contributes to safer, more personalized digital learning experiences.

Zoir Botirov, Lecturer, Department of Psychology, Termez State University, Uzbekistan. He specializes in educational psychology, cognitive behavior, and learner profiling. His research focuses on psychological assessment techniques in digital learning environments. Zoir explores how behavioral patterns can enhance cybersecurity awareness and response. He contributes to integrating psychology into educational technology and digital safety training.

Zilola Yunusova, Senior Teacher, Journalism & Mass Communications University of Uzbekistan. She works on digital safety in media education and cyber journalism. Her interests include misinformation, identity protection, and media profiling. Zilola supports student training in safe communication tools. She researches digital influence and behavioral manipulation in education. Her work promotes journalism ethics in online learning.

Asal Kasimova, Associate Professor, Tashkent State Transport University. PhD in Legal Sciences, focused on public law and digital policy. She integrates legal literacy into cybersecurity and education. Her research supports safe legal communication in online classrooms. Asal promotes governance models for institutional cyber defense. She mentors students in digital legal ethics and academic security.