Multitek Indonesia: Jurnal Ilmiah
Volume: 20 No. .2 December 2026, Hal. 128 - 139
ISSN: 1907-6223 (print)
ISSN: 2579-3497 (Online)
http://journal.umpo.ac.id/index.php/multitek
https://doi.org/10.24269/mtkind.v20i2.14612

Intelligent Human-Centric Cybersecurity Framework For Adaptive Phishing Mitigation In Higher Education Institutions

Lutfiyah Dwi Setia[1,2*], Imam Riadi[3], Herman Yuliansyah[1]
[1] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191
[2] Department of Information Technology, Politeknik Negeri Madiun, Madiun, Indonesia, 63133
[3] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, 55191
Corresponding Author's Email : **2536083036@webmail.uad.ac.id; lutfiyah17@pnm.ac.id**

Received : August 26, 2026 **Revised : September 22, 2026** **Accepted : October 10, 2026**

Abstract

Phishing in higher education combines technical exposure with user-level and organizational vulnerabilities, yet the literature often treats these dimensions separately. This study develops an Intelligent Human-Centric Cybersecurity Framework through a structured narrative review and thematic synthesis. Sources were drawn from Scopus, IEEE Xplore, SpringerLink, and ScienceDirect, with the main search window covering 2021–2026. The review screened 268 candidate records and retained 25 sources represented in the final synthesis. A hybrid deductive–inductive coding procedure was used to examine digital literacy, cybersecurity awareness, organizational security culture, behavioral monitoring, and adaptive response while allowing additional themes such as phishing simulation, user compliance, and security fatigue to emerge. The synthesis indicates that human capability and institutional reinforcement become more actionable when they are connected to behavioral evidence and a feedback mechanism. In the proposed framework, "intelligent" refers to the use of monitoring and analytics to support evidence-informed mitigation decisions, whereas "adaptive" refers to the adjustment of training, policy, or controls in response to observed behavior and evolving phishing patterns. The framework is conceptual rather than empirically validated; therefore, controlled phishing simulations and quantitative model testing are proposed as subsequent validation steps.

Keyword: adaptive cybersecurity, behavioral monitoring, higher education, human-centric cybersecurity, phishing mitigation

Copyright: ©2026 The authors. This article is published by LPPM and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

INTRODUCTION

The expansion of cloud-based academic services, Learning Management Systems (LMS), remote authentication, and online collaboration has increased the digital exposure of higher education institutions. Phishing is particularly relevant in this environment because attackers can exploit both institutional communication channels and users' routine decisions [1]. Awareness training can reduce susceptibility when users learn to recognize suspicious messages, links, and credential requests [2], but the diversity of students, lecturers, staff, researchers, and external collaborators makes phishing resistance difficult to manage through a single technical control.

Human-centric cybersecurity addresses this limitation by treating user behavior, organizational conditions, and technical protection as interdependent elements. In higher education, reporting and

compliance are shaped not only by individual knowledge but also by leadership, policy, peer norms, and security culture [3]–[5]. Behavioral evidence is therefore important because it shows how users actually respond to suspicious interactions rather than relying only on self-reported awareness [6].

Existing research nevertheless remains unevenly distributed. Studies on awareness and security culture emphasize education, policy, and user engagement [7], whereas technical research concentrates on filtering, malicious-URL classification, and machine-learning-based detection [8]. These mechanisms are useful for threat identification but do not fully explain decisions shaped by trust, urgency, persuasion, and other social-engineering cues [9]. This separation between technical detection and human behavior limits the ability to design interventions that change as user risk patterns change.

Higher education also presents a specific governance problem. Universities deliberately maintain relatively open digital ecosystems to support teaching, research, public services, and collaboration. Academic-service security and incident-readiness studies show that governance, service management, and forensic preparation are important to institutional resilience [10], [11]. However, these strands are rarely connected to a human-centered feedback process that uses observed behavior to refine awareness, policy, or technical controls.

The need for adaptation is reinforced by changes in both attacker tactics and defensive technologies. Adversarial phishing research shows that detection models require repeated evaluation as attacks evolve [12], while human-centered cybersecurity research argues that organizational resilience and user behavior should be treated as part of the same security system [13]. Repetitive awareness activities can also produce security fatigue [14], which supports the use of contextual and behavior-oriented education rather than identical training for all users [15].

Behavioral studies provide a theoretical basis for this integration. Phishing susceptibility has been associated with cognition, suspicion, automaticity, persuasion, authority, and emotional response [16], [19], [20]. Security-behavior instruments and information-security culture research further show that knowledge, attitude, organizational norms, and reinforcement influence secure practice [17], [18]. Technical studies on forensics, vulnerability assessment, ransomware detection, and data protection [21]–[25] complement these human-centered findings, but they do not by themselves provide an adaptive model for phishing mitigation in higher education.

Three research gaps follow from this literature. First, digital literacy, awareness, security culture, behavioral monitoring, and adaptive response are usually examined as separate mechanisms rather than as a connected mitigation process. Second, the term “intelligent” is frequently associated with technical detection, while the use of behavioral evidence to guide subsequent human-centered interventions is less clearly specified. Third, higher-education frameworks rarely state how a conceptual model should be operationalized and empirically validated. This study addresses these gaps by synthesizing the literature into an Intelligent Human-Centric Cybersecurity Framework for adaptive phishing mitigation in higher education institutions.

The contribution is conceptual rather than a claim of demonstrated effectiveness. The framework organizes five core components—digital literacy, cybersecurity awareness, organizational security culture, behavioral monitoring, and adaptive response—into a feedback-oriented sequence. It also clarifies that intelligence is evidence-informed support from monitoring and analytics, whereas adaptation is the deliberate modification of training, policy, or controls when observed risk patterns change. The resulting model is intended to guide later implementation and validation in operational academic environments.

RESEARCH METHOD

2.1 Review Design and Search Strategy

This study used a structured narrative literature review with thematic synthesis. A narrative design was retained because the objective was conceptual integration rather than pooled effect estimation, but the search and screening process was made explicit to improve transparency and replicability. The review examined human-centered factors in phishing mitigation, with attention to digital literacy, cybersecurity awareness, organizational security culture, behavioral monitoring, adaptive response, and related mechanisms [2], [7], [15].

Sources were searched in Scopus, IEEE Xplore, SpringerLink, and ScienceDirect. The main publication window was 2021–2026, while older sources were retained only when they provided foundational constructs or established behavioral/security models. The standardized Boolean expression used to operationalize the search scope was: ("phishing" OR "social engineering") AND ("higher education" OR universit* OR college*) AND ("human-centric" OR "human centered" OR "cybersecurity awareness" OR "digital literacy" OR "security culture" OR "behavioral monitoring" OR "adaptive cybersecurity"). The same conceptual expression was applied across the four databases, with field syntax adapted to the search interface.

At aggregate level, 268 candidate records were screened against the review scope. Studies were eligible when they were scholarly publications with a clear relationship to phishing/social engineering, human or organizational cybersecurity, adaptive mitigation, or higher-education security; empirical studies also needed a traceable description of data and analysis. Records were excluded when they were duplicates, outside the phishing/human-centric scope, purely technical without relevance to the conceptual model, or insufficiently documented for thematic interpretation. Twenty-five sources represented in the final reference set were retained for synthesis, and 243 candidate records were excluded during screening and eligibility assessment. Figure 1 summarizes this simplified selection process.

Thematic coding combined deductive and inductive procedures. The deductive pass used seed categories supported by prior work on awareness, training, and human behavior [2], [7], [15]. A separate open-coding pass was then used to retain recurring concepts that did not fit the initial categories. This inductive step produced additional themes—including phishing simulation, user compliance, security fatigue, and feedback-driven intervention—which were preserved rather than forced into the original five-component structure. A final comparison mapped the resulting themes to capability, institutional reinforcement, behavioral evidence, and adaptive response.

Quality and credibility were screened at the publication-reporting level before a source was used as thematic evidence. The appraisal considered: (1) clarity of the research objective or conceptual proposition; (2) transparency of the reported method or theoretical basis; (3) traceability of findings or arguments to data/literature; and (4) direct relevance to at least one framework component. Empirical evidence was distinguished from conceptual or review evidence so that conceptual publications were not treated as proof of behavioral effectiveness. Among the 25 retained sources, 18 were classified as empirical primary studies, three as reviews/surveys, and four as conceptual or foundational contributions.

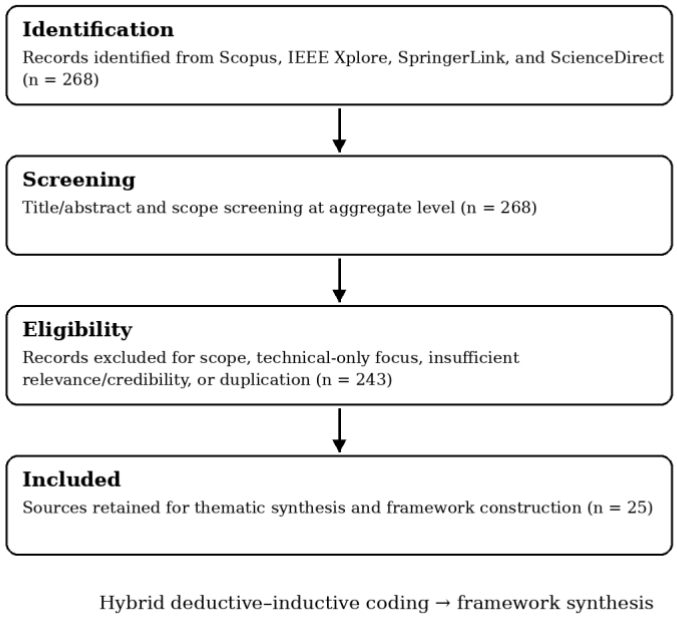


Figure 1. Simplified review-selection and framework-synthesis flow.

2.2 Evidence Scope and Study-Type Distribution

The retained evidence set covered phishing attacks, cybersecurity awareness, digital literacy, security culture, user behavior, intelligent detection, and adaptive security. Primary empirical studies constituted 18 of the 25 retained sources (72%), reviews or surveys accounted for three (12%), and conceptual/foundational publications accounted for four (16%). The empirical group supplied evidence about user behavior, detection, validation, governance, or forensic/security practice, while reviews and conceptual publications were used mainly to establish constructs, recurring issues, and integration logic.

Most evidence used for contemporary synthesis was drawn from 2021–2026. Earlier publications were retained selectively when they defined constructs still used in current research, including phishing susceptibility, information-security culture, persuasion, and human aspects of information security [16]–[20]. This distinction prevents older foundational work from being interpreted as direct evidence of current higher-education conditions.

2.3 Hybrid Thematic Analysis

The thematic synthesis examined both the recurrence and the function of human-centered factors. Six analytical areas were used during the final comparison: cybersecurity awareness, digital literacy, organizational security culture, behavioral monitoring, adaptive security mechanisms, and phishing-resistance behavior. These areas reflect evidence that phishing susceptibility is influenced by cognition, persuasion, automaticity, social-engineering cues, and user security behavior in addition to technical protection [16], [19], [20].

Coding emphasized observable or actionable aspects. Awareness captured recognition and response to suspicious email features; digital literacy captured critical evaluation of online information and identities; security culture captured management support, policy, compliance, and reporting; and behavioral monitoring captured evidence from user interactions or activity logs [4], [5], [11], [18]. Open coding additionally identified simulation, compliance, security fatigue, and feedback as cross-cutting themes that help explain how the main components can be linked.

Behavioral monitoring was interpreted as the evidence layer of the model, while adaptive response was interpreted as the mechanism that turns evidence into changed action. In practical terms, observed errors, reporting behavior, simulated-phishing outcomes, or repeated risk patterns can inform

the selection of follow-up training, policy adjustment, or technical controls. The synthesis therefore evaluated not only whether a factor appeared in the literature but also what role it could play in a closed feedback cycle [6], [11].

2.4 Framework Construction and Construct Definitions

The framework was constructed from five components that recurred across the reviewed evidence: digital literacy, cybersecurity awareness, organizational security culture, behavioral monitoring, and adaptive response. The first three represent user capability and institutional reinforcement; behavioral monitoring supplies evidence about actual behavior; and adaptive response defines how mitigation changes in response to that evidence. These relationships form the core of the Intelligent Human-Centric Cybersecurity Framework.

Within the model, “intelligent” does not imply autonomous decision making. It refers to the use of monitoring, analytics, simulation results, and other behavioral evidence to support targeted security decisions. “Adaptive” refers to a feedback process in which interventions are revised when user behavior or threat patterns change. Digital literacy and awareness support recognition and evaluation, security culture reinforces expected behavior, monitoring observes outcomes, and adaptive response closes the loop by modifying training, policy, or technical safeguards.

This structure is consistent with research that combines human-centered cybersecurity, organizational resilience, adaptive defense, and academic security governance [3], [10], [13]. Figure 2 presents the conceptual relationships. Because the framework has not yet been tested empirically, its arrows represent synthesized propositions rather than validated causal effects.

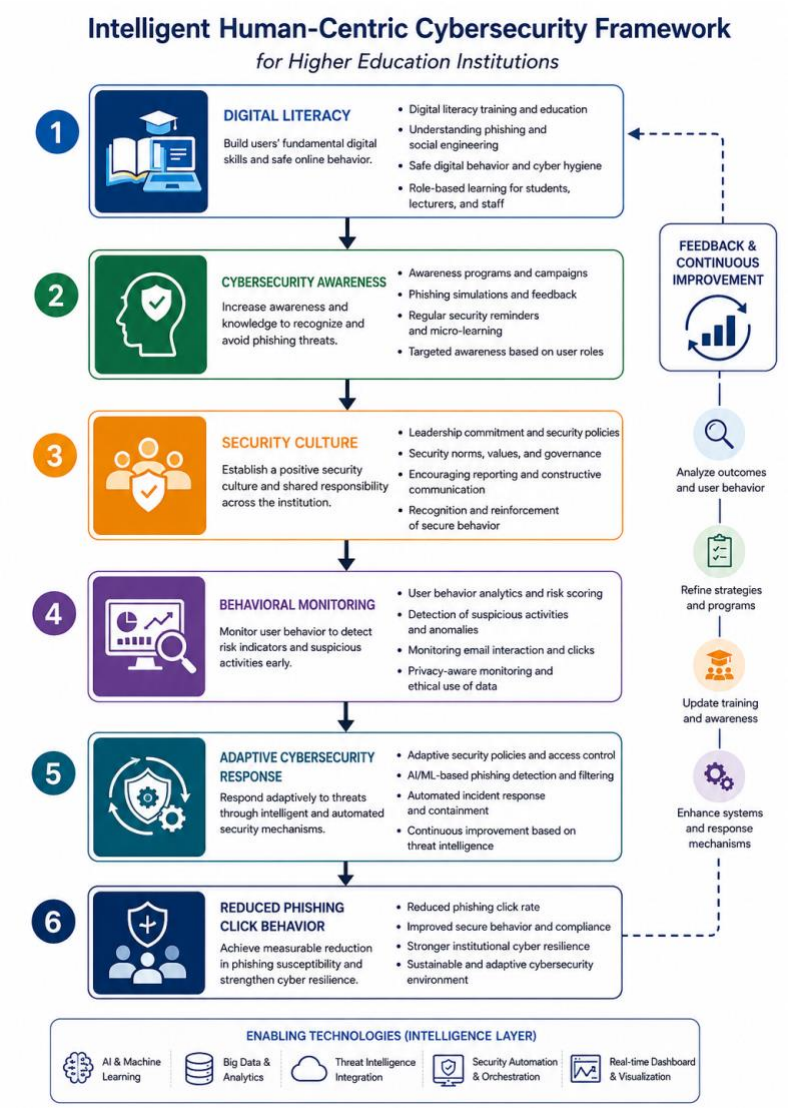


Figure 2. Intelligent Human-Centric Cybersecurity Framework.

2.5 Synthesis Logic

The final synthesis organized the evidence into four functional layers: capability, reinforcement, observation, and response. Digital literacy and cybersecurity awareness form the capability layer; security culture provides institutional reinforcement; behavioral monitoring provides observation; and adaptive response converts observed patterns into modified mitigation. Phishing simulation, user compliance, and security fatigue were retained as cross-cutting themes because they influence more than one layer.

This functional arrangement avoids treating the five components as independent predictors with assumed statistical significance. Instead, the framework represents a conceptual sequence derived from recurring relationships reported in the literature. Awareness and digital literacy support threat recognition, security culture supports sustained behavior, monitoring provides evidence, and adaptive response uses that evidence to revise intervention [4], [5], [14]–[20].

The resulting feedback loop is the principal synthesis of the review: human behavior is both an object of protection and a source of evidence for the next mitigation decision. This relationship provides the conceptual bridge between human-centered governance and intelligent security mechanisms.

RESULTS AND DISCUSSION

The results are presented as a synthesis of the retained evidence rather than as effect-size estimates. The review screened 268 candidate records and retained 25 sources for thematic synthesis. The corpus consisted of 18 empirical primary studies, three reviews/surveys, and four conceptual or foundational publications. The sections below report the evidence by function and then integrate it into the proposed framework.

3.1 Study Selection and Corpus Profile

The aggregate screening process excluded 243 candidate records that did not meet the stated relevance, eligibility, or credibility criteria. The final 25-source corpus was intentionally heterogeneous because the framework requires evidence at several levels: user behavior, awareness and literacy, organizational culture, monitoring, adaptive response, and technical context. Empirical sources were used to support behavioral or operational claims, whereas review and conceptual sources were used to define constructs and integration logic.

3.2 Thematic Synthesis of Human-Centric Cybersecurity Factors

The synthesis identified seven recurring human-centered themes. Rather than assigning unsupported statistical "impact levels," Table 1 summarizes the conceptual role of each theme and cites representative evidence used in the synthesis. The five core framework components are complemented by phishing simulation and user compliance, which function as cross-cutting implementation themes.

Table 1. Thematic synthesis of human-centric cybersecurity factors

Factor	Synthesized Role	Framework Function	Representative Evidence
Cybersecurity Awareness	Recognize and respond to phishing cues	User capability	[2], [4], [7], [15], [17]
Digital Literacy	Evaluate digital information, identities, and links	User capability	[1], [9], [16], [20]
Security Culture	Reinforce reporting, compliance, and shared norms	Institutional reinforcement	[4], [5], [18]
Behavioral Monitoring	Observe interaction patterns and recurring risk	Evidence layer	[6], [11], [12]
Adaptive Awareness Training	Adjust learning to observed weaknesses	Adaptive intervention	[2], [7], [14], [15]
User Compliance	Translate policy and norms into routine behavior	Cross-cutting outcome	[4], [5], [17], [18]
Phishing Simulation	Provide controlled behavioral evidence and feedback	Cross-cutting mechanism	[2], [7], [13], [15]

The table distinguishes what each theme contributes to the framework rather than treating recurrence as evidence of causal strength. This is important because the reviewed studies use different populations, methods, and outcome measures, so the synthesis supports conceptual relationships but not a pooled estimate of effect.

Awareness and digital literacy primarily contribute to user capability, while security culture operates at the institutional level. Behavioral monitoring and phishing simulation provide observable evidence that can be used to refine interventions. This functional differentiation is the basis for the framework architecture rather than a claim that one factor is universally more important than another.

Phishing simulation is especially relevant to the adaptive component because it produces behavioral observations under controlled conditions. When linked to reporting, click behavior, or other risk indicators, simulation can support targeted follow-up rather than one-size-fits-all training.

3.3 Cybersecurity Awareness Synthesis

Cybersecurity awareness was operationalized in the literature through recognition and response behaviors, including identification of suspicious email characteristics, URL checking, credential

protection, and policy compliance. Table 2 links these indicators to representative evidence rather than presenting them as experimentally proven effects across all settings.

Table 2. Cybersecurity awareness indicators and evidence basis

Indicator	Interpretation in the Synthesis	Representative Evidence
Email Recognition	Recognition of suspicious message features	[2], [7], [15]
URL Validation	Verification before link interaction	[1], [2], [9]
Credential Protection	Protection against credential-harvesting attempts	[2], [17]
Security Compliance	Following institutional guidance and reporting practices	[4], [5], [18]

The evidence supports repeated and contextualized awareness activity rather than a single exposure. However, the review does not treat awareness as sufficient on its own; its practical value increases when user responses are observed and connected to subsequent simulation, feedback, or institutional reinforcement [2], [7], [15].

This relationship links awareness to the feedback cycle: monitoring or simulation identifies recurring errors, and the next intervention can focus on the specific recognition or response problem that was observed.

3.4 Digital Literacy Synthesis

Digital literacy complements cybersecurity awareness by emphasizing evaluation rather than threat recall. Relevant skills include checking website legitimacy, inspecting message context, validating information, and understanding authentication practices. These functions are summarized in Table 3 together with the evidence used to connect them to phishing-related decision making.

Table 3. Digital literacy components and evidence basis

Component	Role in Phishing Mitigation	Representative Evidence
URL Verification	Evaluate legitimacy before interaction	[1], [9], [16]
Email Inspection	Interpret suspicious message cues and context	[1], [16], [20]
Information Validation	Question authenticity and persuasive claims	[9], [19], [20]
Authentication Awareness	Apply safer identity and credential practices	[2], [17]

The literature supports a conceptual link between stronger evaluation skills and more cautious interaction with suspicious content, but the included studies use different measures and populations. The framework therefore treats digital literacy as a user-capability construct to be tested empirically rather than as a confirmed universal predictor.

In implementation, digital-literacy activities can be tied to realistic verification tasks so that users practice checking identities, URLs, and contextual claims that commonly appear in phishing messages.

3.5 Organizational Security Culture Synthesis

Organizational security culture represents the conditions that make secure behavior expected, supported, and repeatable. The reviewed evidence emphasizes management support, policy enforcement, shared awareness, and monitoring as mechanisms that can reinforce reporting and compliance. Table 4 summarizes these elements and their evidence basis.

Table 4. Organizational security culture indicators and evidence basis

Indicator	Role in the Framework	Representative Evidence
Management Support	Legitimizes security priorities and resources	[4], [5]
Security Policy Enforcement	Establishes expected security behavior	[5], [10], [18]
Organizational Awareness	Creates shared norms and responsibility	[4], [5], [18]
Continuous Monitoring	Supplies feedback for governance and intervention	[6], [11]

The synthesis suggests that culture is the mechanism that embeds awareness and reporting in routine institutional practice. This interpretation does not assume a direct causal effect; rather, it identifies organizational support as the context in which user-level interventions are more likely to be sustained [4], [5], [18].

For the proposed framework, security culture therefore serves as the bridge between individual capability and institution-wide response, ensuring that feedback from monitoring can lead to policy, communication, or training changes.

3.6 Cross-Theme Synthesis and Emerging Themes

Cross-theme comparison showed that the five core components perform different but complementary functions. Awareness and digital literacy build user capability; security culture reinforces expected behavior; monitoring makes behavior observable; and adaptive response changes mitigation based on that evidence. Inductive coding also retained phishing simulation, user compliance, security fatigue, and feedback as emerging themes. These themes were not forced into separate framework components because they operate across multiple stages—for example, simulation provides evidence, compliance reflects institutional reinforcement, and security fatigue affects how adaptive training should be designed.

3.7 Proposed Intelligent Human-Centric Cybersecurity Framework

The proposed framework integrates the synthesis into a continuous cycle: digital literacy → cybersecurity awareness → organizational security culture → behavioral monitoring → adaptive response → revised mitigation. The arrows in Figure 3 represent conceptual relationships derived from the literature, not statistically validated causal paths.

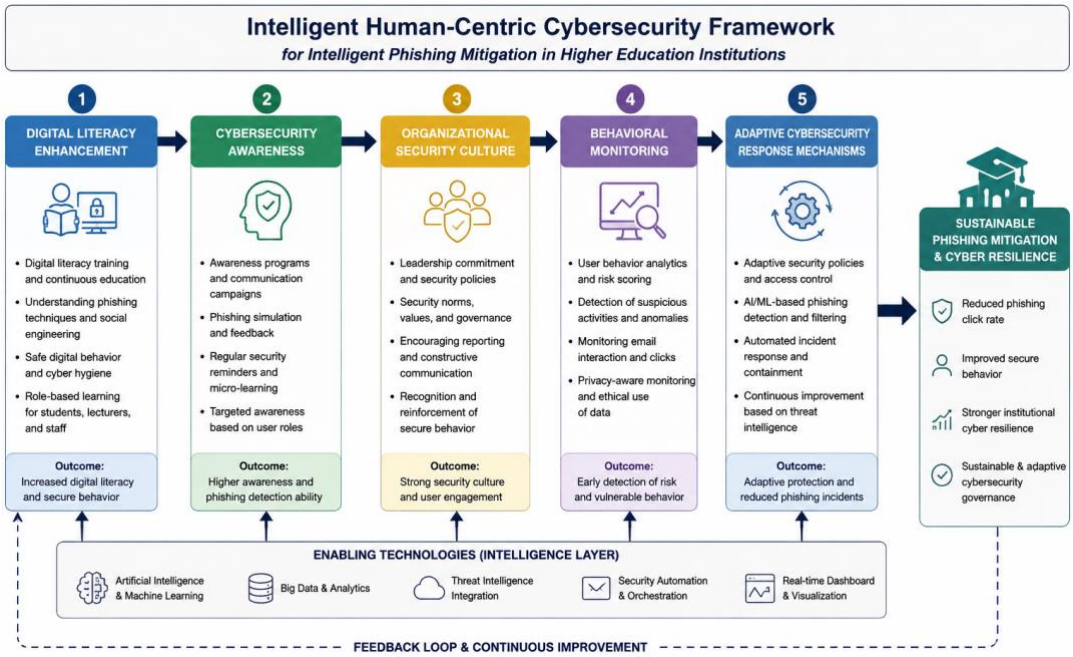


Figure 3. Intelligent Human-Centric Cybersecurity Framework for Adaptive Phishing Mitigation in Higher Education Institutions.

The framework combines human capability, organizational reinforcement, and technical feedback. Digital literacy and awareness support recognition and evaluation; security culture reinforces reporting and secure practice; behavioral monitoring records actual interaction patterns; and adaptive response uses those patterns to revise mitigation. In this sense, the "intelligent" layer assists evidence-informed decisions through analytics, monitoring, or simulation data, while the "adaptive" layer changes intervention based on the resulting evidence.

Adaptive response is the transition from observation to action. Depending on the observed pattern, an institution may change simulation difficulty, target a specific user group with additional training, revise reporting procedures, adjust communication, or strengthen a technical control. Cyber-profiling research demonstrates that user activity logs can support the identification of recurring patterns in higher-education networks [11]. The framework uses such evidence to support, rather than replace, human security judgment.

3.8 Implementation and Empirical Validation Pathway

Implementation can begin with a baseline assessment of digital literacy, cybersecurity awareness, and perceived security culture, followed by a controlled phishing-simulation wave that records behavioral outcomes such as message opening, link interaction, reporting, or ignored messages. Monitoring data can then be used to define risk patterns and select targeted interventions. A subsequent simulation wave can test whether the intervention changes behavior. This sequence operationalizes the framework's feedback loop without requiring fully autonomous decision making.

Empirical validation should test both the measurement of the human-centered constructs and the behavioral outcomes of the adaptive cycle. Structural Equation Modeling (SEM) or Partial Least Squares Structural Equation Modeling (PLS-SEM) can evaluate relationships among digital literacy, awareness, security culture, and phishing-resistance constructs, while controlled phishing simulations provide observed behavioral measures. A multi-university design would allow the framework to be tested across different governance contexts and user populations. Until such validation is completed, the framework should be interpreted as a conceptual model and implementation guide.

3.9 Discussion

The synthesis does not support a simple technical-versus-human distinction. Technical controls remain necessary, but phishing succeeds by exploiting decisions that occur after a message reaches a user. The reviewed evidence therefore supports a layered interpretation in which filtering and detection are complemented by user capability, organizational reinforcement, behavioral feedback, and adaptive intervention.

Cybersecurity awareness, digital literacy, and security culture appear repeatedly in the retained literature, but their roles differ. Awareness supports recognition, digital literacy supports evaluation, and security culture determines whether safe practices are institutionally reinforced. Monitoring and simulation contribute a different type of evidence because they observe behavior rather than self-reported knowledge.

The synthesis also clarifies the terms "intelligent" and "adaptive." Intelligence refers to the use of behavioral data and analytical tools to support a mitigation decision; adaptation refers to changing the intervention in response to those observations. This distinction reduces the risk of overclaiming autonomous intelligence and makes the proposed contribution testable in later empirical work.

For higher education, the main practical implication is that awareness programs should not operate independently from governance and behavioral evidence. Monitoring can identify recurring risk patterns, governance determines the available institutional response, and adaptive intervention allows training or controls to be adjusted to the problem that was actually observed.

Conceptually, the framework extends human-centric cybersecurity by making the feedback relationship explicit: user behavior is not only an outcome of mitigation but also an input to the next mitigation decision. This is the main conceptual novelty of the proposed model.

3.10 Research Implications

The framework has two implications. For research, it provides a structure for testing whether user capability, organizational reinforcement, behavioral evidence, and adaptive response operate as an integrated phishing-mitigation process. For practice, it offers a sequence for linking awareness

programs and simulations to observable behavior and institutional policy. Its use as a planning reference is appropriate, but claims of effectiveness should be reserved for future empirical validation.

Accordingly, the framework should be treated as a testable conceptual architecture for adaptive cybersecurity governance in higher education rather than as a validated predictive model.

3.11 Study Limitations

This study has three principal limitations. First, the framework is based on a narrative thematic synthesis rather than a formal systematic review or meta-analysis. Second, the retained sources are methodologically heterogeneous and include empirical, review, and conceptual publications; therefore, the synthesis does not estimate pooled effect sizes or causal strength. Third, the framework has not yet been validated with observed phishing behavior in a higher-education population. These limitations motivate the implementation and validation pathway described above.

CONCLUSION

This study addresses a specific gap in higher-education phishing research: the separation of user capability, institutional security culture, behavioral evidence, and adaptive intervention. Through a structured narrative review and hybrid thematic synthesis, the evidence was organized into five core components—digital literacy, cybersecurity awareness, organizational security culture, behavioral monitoring, and adaptive response—supported by cross-cutting themes such as simulation, compliance, and security fatigue.

The resulting Intelligent Human-Centric Cybersecurity Framework defines intelligence as evidence-informed support from monitoring and analytics, and adaptation as the revision of training, policy, or controls in response to observed behavior and changing threat patterns. This definition positions the framework as a conceptual architecture rather than a validated causal model and reduces the risk of overclaiming its current maturity.

Future work should implement the feedback cycle in operational higher-education environments using controlled phishing simulations, behavioral monitoring, and targeted interventions. Such studies should compare behavioral outcomes across successive simulation waves and examine whether adaptive intervention produces measurable improvement relative to standard awareness activity.

Quantitative validation can combine SEM or PLS-SEM for the human-centered constructs with observed click, report, or ignore behavior from controlled simulations. Multi-university replication would also help determine which relationships are stable across institutions and which require adaptation to local governance, technology, and user populations.

ACKNOWLEDGEMENTS

The authors acknowledge the academic support provided by the Doctoral Program in Informatics, Universitas Ahmad Dahlan, and Politeknik Negeri Madiun. They also appreciate the comments from supervisors, colleagues, and reviewers that helped refine the manuscript.

Generative AI tools were used only for language editing, formatting support, and figure presentation. Literature selection, thematic analysis, interpretation, and verification of the scientific content were carried out by the authors, who take responsibility for the final manuscript.

REFERENCES

[1] E. Morrow, “Scamming higher ed: An analysis of phishing content and trends,” Computers in Human Behavior Reports, vol. 14, p. 100411, 2024, doi: 10.1016/j.chb.2024.108274.

[2] S. Chaudhary, V. Gkioulos, and S. Katsikas, “Developing metrics to assess the effectiveness of cybersecurity awareness program,” Journal of Cybersecurity, vol. 8, no. 1, p. tyac006, 2022, doi: 10.1093/cybsec/tyac006.

[3] A. Gavaza, B. Kandiero, and C. Katsande, “A human-centric cybersecurity framework for ensuring cybersecurity readiness in universities,” in Effective Cybersecurity Operations for Enterprise-Wide Systems, IGI Global, 2023, pp. 242–276, doi: 10.4018/978-1-6684-9018-1.ch012.

[4] R. Armas and H. Taherdoost, "Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm," Information, vol. 16, no. 5, p. 336, 2025, doi: 10.3390/info16050336.
[5] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," Computers & Security, vol. 109, p. 102387, 2021, doi: 10.1016/j.cose.2021.102387.
[6] Z. Fan, X. Li, and Y. Zhang, "Investigation of phishing susceptibility with explainable artificial intelligence," Future Internet, vol. 16, no. 1, p. 31, 2024, doi: 10.3390/fi16010031.
[7] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," Computer Science Review, vol. 40, p. 100361, 2021, doi: 10.1016/j.cosrev.2021.100361.
[8] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," Neural Computing and Applications, vol. 28, no. 12, pp. 3629–3654, 2017, doi: 10.1007/s00521-016-2275-y.
[9] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," Human-centric Computing and Information Sciences, vol. 8, no. 1, p. 5, 2018, doi: 10.1186/s13673-018-0128-7.
[10] I. Riadi, I. T. Riyadi Yanto, and E. Handoyo, "Cyber security analysis of academic services based on domain delivery services and support using Indonesian e-government ratings (PEGI)," Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, vol. 5, no. 4, pp. 263–270, 2020, doi: 10.22219/kinetik.v5i4.1083.
[11] M. Zulfadhilah, Y. Prayudi, and I. Riadi, "Cyber profiling using log analysis and K-means clustering: A case study higher education in Indonesia," International Journal of Advanced Computer Science and Applications, vol. 7, no. 7, pp. 430–435, 2016.
[12] A. Kulkarni, V. Balachandran, D. M. Divakaran, and T. Das, "Evaluating the robustness of phishing webpage detection models against adversarial attacks," Computers & Security, vol. 142, p. 103987, 2024, doi: https://doi.org/10.48550/arXiv.2407.20361
[13] M. Jalali, J. Bruckes, and M. Westmattelmann, "Why employees still click on phishing links: Investigation in hospitals," Journal of Medical Internet Research, vol. 22, no. 1, p. e16775, 2020, doi: 10.2196/16775.
[14] S. Furnell and K. Thomson, "Recognising and addressing 'security fatigue'," Computer Fraud & Security, vol. 2021, no. 11, pp. 5–10, 2021, doi: https://doi.org/10.1016/S1361-3723(09)70139-3.
[15] P. Kirlappos and M. A. Sasse, "Security education against phishing: A modest proposal for a major rethink," IEEE Security & Privacy, vol. 20, no. 2, pp. 72–77, 2022, doi: 10.1109/MSP.2011.179
[16] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Suspicion, cognition, and automaticity model of phishing susceptibility," Communication Research, vol. 45, no. 8, pp. 1146–1166, 2018, doi: 10.1177/0093650215627483.
[17] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," Computers & Security, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.
[18] A. AlHogail, "Design and validation of information security culture framework," Computers in Human Behavior, vol. 49, pp. 567–575, 2015, doi: 10.1016/j.chb.2015.03.054.
[19] M. Workman, "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," Journal of the American Society for Information Science and Technology, vol. 59, no. 4, pp. 662–674, 2008, doi: 10.1002/asi.20779.
[20] A. Ferreira and R. Teles, "Persuasion: How phishing emails can influence users and bypass security mechanisms," International Journal of Human-Computer Studies, vol. 125, pp. 19–31, 2019, doi: 10.1016/j.ijhcs.2018.12.004.
[21] R. Umar, I. Riadi, and R. S. Kusuma, "Analysis of Conti ransomware attack on computer network with live forensic method," International Journal on Informatics for Development, vol. 10, no. 1, pp. 53–61, 2021, doi: 10.14421/ijid.2021.2423.
[22] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using Open Web Application Security Project (OWASP) framework," Journal of Theoretical and Applied Information Technology, vol. 95, no. 6, pp. 1363–1371, 2017.
[23] A. Kurniawan and I. Riadi, "Detection and analysis Cerber ransomware based on network forensics behavior," International Journal of Network Security, vol. 20, no. 5, pp. 836–843, 2018, doi: 10.6633/IJNS.201809.20(5).04.
[24] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data security for school service top-up transactions based on AES combination blockchain technology modification," Lontar Komputer: Jurnal Ilmiah Teknologi Informasi, vol. 11, no. 3, pp. 155–166, 2020, doi: 10.24843/LKJITI.2020.v11.i03.p04.
[25] Sunardi, I. Riadi, and P. A. Raharja, "Vulnerability analysis of e-voting application using Open Web Application Security Project (OWASP) framework," International Journal of Advanced Computer Science and Applications, vol. 10, no. 11, pp. 135–142, 2019.