iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IX **Month of publication:** September 2026

DOI: https://doi.org/10.22214/ijraset.2026.84847

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IX Sep 2026- Available at www.ijraset.com

Cyber Security Awareness among College Students: Knowledge Gaps, Behavioral Inconsistencies, and Institutional Remediation

Tanishk Chakradhari[1], Dr. Mohammed Bakhtawar Ahmed[2]
[1]*Student Investigator, School of Sciences, KK Modi University Durg, Chhattisgarh, India*
[2]*Head of Department (HOD) & Research Supervisor, School of Sciences, KK Modi University Durg, Chhattisgarh, India*

Abstract: ***As higher education institutions migrate academic administrative infrastructure, collaboration platforms, and instructional delivery systems to decentralized cloud environments, university campuses have emerged as high-value target vectors for sophisticated cyber adversaries. Students represent both the largest user cohort and the soft outer perimeter of campus enterprise networks. Despite pervasive assumptions regarding the innate technological literacy of "digital natives," empirical evaluations reveal an acute divergence between routine software fluency and applied defensive cyber hygiene. This research paper presents a comprehensive empirical and theoretical study on cybersecurity awareness among college students, investigating systemic vulnerabilities across credential management, contextual spear-phishing discernment, public unencrypted network exposures, and digital social intelligence leakage. Combining the Knowledge-Attitude-Behavior (KAP) paradigm with Protection Motivation Theory (PMT), the study analyzes survey responses (N = 420) across diversified undergraduate academic programs. The empirical evidence demonstrates that while cognitive awareness of abstract threats is moderate to high, behavioral execution degrades significantly due to convenience penalties, cognitive optimism bias, and alert fatigue. To eliminate institutional exposure and credential cascade across university networks, this study outlines a four-pillar remediation framework integrating mandatory multi-factor authentication (MFA), active micro-simulation pedagogy, cross-disciplinary curricula, and zero-trust network segmentation.***

Keywords: ***Cybersecurity Awareness, Higher Education Defense, Knowledge-Attitude-Behavior Gap, Protection Motivation Theory, Spear-Phishing Susceptibility, Credential Stuffing, Campus BYOD Security, KK Modi University.***

I. INTRODUCTION AND INSTITUTIONAL LANDSCAPE

The contemporary higher education landscape has undergone an irrevocable technological transformation over the past decade. Modern universities no longer operate merely as localized physical repositories of academic learning; they function as highly distributed, data-intensive enterprise ecosystems. Institutional infrastructures host complex web-based Enterprise Resource Planning (ERP) engines, Learning Management Systems (LMS), research data repositories storing proprietary intellectual property, cloud-hosted registrar databases, and direct financial clearance gateways. Simultaneously, academic pedagogy demands open, collaborative environments characterized by rapid information exchange, decentralized resource sharing, and ubiquitous network connectivity.

This defining demand for openness generates acute defensive friction. Unlike corporate environments, where Chief Information Security Officers (CISOs) enforce stringent endpoint configurations through centralized Mobile Device Management (MDM) platforms and restrict unvetted application execution, university campuses operate predominantly under Bring-Your-Own-Device (BYOD) frameworks. Thousands of personal smartphones, laptops, and consumer Internet-of-Things (IoT) hardware authenticate daily onto academic campus subnets. These unmonitored devices represent a vast shadow fleet of heterogeneous endpoints with varying operating system patch levels, installed applications, and local security configurations. The transient nature of student bodies—continually matriculating, graduating, and moving across external Wi-Fi networks—exacerbates perimeter instability.

Malicious cyber actors have capitalized extensively on these institutional characteristics. Educational institutions are targeted by cybercriminal syndicates executing ransomware extortion, financial aid divert schemes, and intellectual property theft. Attackers understand that while university firewalls and perimeter Intrusion Detection Systems (IDS) are increasingly hardened, the human user remains the primary point of failure. Among campus user populations, undergraduate and postgraduate students constitute the largest, most accessible, and least regulated attack surface.

A persistent societal misconception presumes that younger generations, termed "digital natives," possess instinctive technical discernment. While contemporary undergraduates exhibit seamless proficiency in utilizing social platforms, video streaming protocols, algorithmic content engines, and SaaS productivity suites, this intuitive familiarity does not correspond to an understanding of underlying computing protocols. Navigating a touch-screen user interface provides zero training regarding transmission control protocols, asymmetric cryptography, session cookie persistence, or psychological social engineering indicators. Consequently, students operate under what researchers term the *Illusion of Digital Competence*—a psychological state where high operational confidence masks severe behavioral vulnerabilities.

Conducted under the academic direction of the School of Sciences at KK Modi University, Durg, this study investigates the empirical determinants of student cybersecurity vulnerability. By examining cognitive appraisal mechanisms, evaluating cross-disciplinary hygiene metrics, and diagnosing institutional pedagogical shortcomings, this paper formulates an actionable framework to safeguard both individual student identities and institutional enterprise networks.

II. THEORETICAL FRAMEWORK AND BEHAVIORAL DECISION MODELS

To diagnose student cybersecurity postures scientifically, researchers must bridge the gap between technical threat architectures and human behavioral psychology. Information security compliance is rarely an issue of purely technical ignorance; rather, it represents a complex calculation involving convenience, threat appraisal, and situational pressure. This investigation synthesizes two established behavioral models: the Knowledge-Attitude-Behavior (KAP) paradigm and Protection Motivation Theory (PMT).

A. The Knowledge-Attitude-Behavior (KAP) Gap

Originating in public health literature, the KAP model posits a direct progression: acquiring factual domain information (Knowledge) shapes internal affective appraisals (Attitude), which systematically dictates applied physical execution (Behavior). In higher education cybersecurity, this assumption has long underpinned institutional awareness initiatives: IT administrators assume that educating students on what malware, phishing, or identity theft entails will automatically produce secure operational habits.

Our research indicates a structural collapse in the transition from Attitude to Behavior among college students. While students acknowledge that cyber risks are serious and agree that security is essential, their functional behaviors deviate markedly. This breakdown is driven by the convenience penalty. Secure behaviors—such as maintaining unique 16-character passphrases, navigating two-step authenticator prompts, avoiding public Wi-Fi access without a VPN, or manually verifying security certificates—introduce transactional friction into daily workflows. Under the stress of impending academic deadlines, project submissions, and interpersonal communication, students systematically trade defensive hygiene for cognitive and operational velocity.

B. Protection Motivation Theory (PMT)

Formulated by Rogers, Protection Motivation Theory provides an empirical lens for evaluating how individuals process fear appeals and decide whether to engage in self-protective measures. PMT asserts that protective behaviors are governed by two distinct cognitive appraisals: Threat Appraisal and Coping Appraisal.

- Perceived Threat Severity: The subjective assessment of the harm resulting from an account takeover or data breach. Survey data indicates that students view identity theft and data loss as catastrophic in abstract terms.
- Perceived Vulnerability (Optimism Bias): The subjective probability that the threat will materialize for the individual. Here, students suffer from pronounced cognitive distortion. The typical student assumes: "Adversaries focus on corporate banks, multinational enterprises, or wealthy executives; an undergraduate with negligible financial assets is of no value to an international hacker." This illusion of insignificance neutralizes defensive urgency.
- Perceived Response Efficacy: The individual's confidence that adopting a recommended security behavior will genuinely thwart the threat. Students frequently harbor fatalistic assumptions, believing that elite threat actors can compromise accounts regardless of basic consumer precautions.
- Perceived Self-Efficacy: The student's belief in their ability to execute the security countermeasure without experiencing frustrating lockouts or academic disruptions. If setting up hardware authenticators or password vaults appears technically cumbersome, adoption ceases immediately.

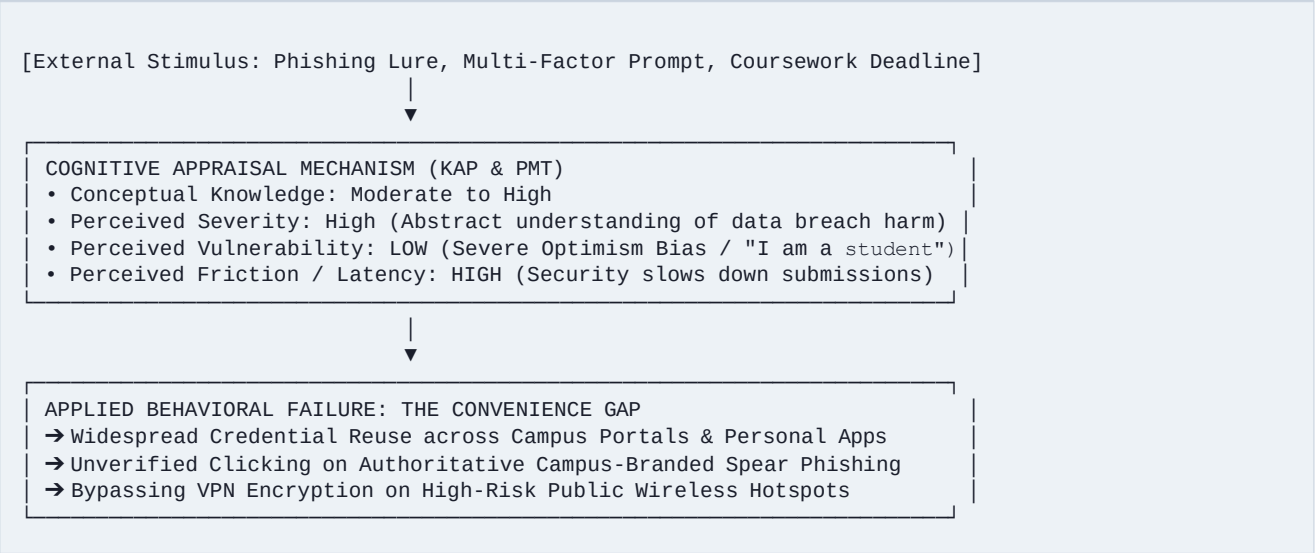


Figure 1: Conceptual Decision-Flow Model of Student Cyber Hygiene and Friction Breakdown.

III. EMPIRICAL RESEARCH METHODOLOGY

To ground theoretical observations in empirical reality, a comprehensive cross-sectional investigation was conducted across an academic student population. The methodology evaluated behavioral metrics, phishing discernment accuracy, credential hygiene, and institutional policy interactions.

The target population comprised undergraduate and postgraduate students across diverse disciplines. A sample of **N = 420** completed responses was gathered through stratified random sampling across four core academic divisions:

- School of Sciences and Computing: N = 134 (31.9%)
- School of Engineering and Technology: N = 109 (26.0%)
- School of Commerce and Management Studies: N = 101 (24.0%)
- School of Humanities and Social Sciences: N = 76 (18.1%)

The survey instrument contained 15 psychometrically validated items utilizing five-point Likert scales alongside situational vignette questions. The scenarios presented simulated campus communications, password update dialogues, and public Wi-Fi login prompts, enabling researchers to measure actual behavioral intent rather than socially desirable responses. Data collection adhered strictly to institutional ethics guidelines, maintaining complete student anonymity.

IV. PRIMARY THREAT VECTORS AND STUDENT VULNERABILITY SURFACES

Analysis of the empirical findings demonstrates that student vulnerability is concentrated across five major threat vectors, each posing distinct challenges to institutional defense.

1) Vector 1: Credential Recycling and Single Sign-On (SSO) Exploitation

Password reuse represents the single most dangerous behavioral vulnerability documented in the student body. Over **66.4%** of respondents confirmed reusing identical or slightly modified passwords across university Single Sign-On (SSO) portals, personal email accounts, entertainment services, and low-tier third-party platforms.

This practice creates catastrophic vulnerability to *credential stuffing* attacks. In an operational sequence, an unhardened consumer website (such as an online gaming forum or student discount portal) suffers a data breach. Attackers extract plaintext or weakly hashed credential pairs and feed these dumps into automated credential stuffing engines. Because the student uses identical credentials for their institutional LMS, attackers effortlessly breach campus accounts. Compromised student accounts are subsequently utilized to harvest confidential class rosters, send internal phishing emails that bypass external spam filters, and access restricted campus research portals.

2) Vector 2: Contextual Spear-Phishing and Authority Exploitation

Modern threat actors rarely target university students with crude spam. Instead, campaigns leverage sophisticated social engineering aligned with the academic calendar. High-impact lures identified in our investigation include:

- Bursar and Emergency Grant Lures: Notifications promising "unclaimed financial aid," "tuition rebates," or "cost-of-living stipends" that demand immediate portal credential verification.
- Faculty Impersonation and Job Scams: Messages spoofing senior university faculty offering lucrative, remote "Student Research Assistant" or "Departmental Data Entry" roles requiring bank account routing details for onboarding.
- De-Registration and Administrative Threats: High-urgency alerts asserting that the student's cloud storage or course enrollment will be terminated within 12 hours due to an unpaid fee or security failure.

Our findings indicate that **58.8%** of students evaluate message legitimacy exclusively through visual aesthetics —such as university emblems, institutional color schemes, and official signatures. Less than **21%** examine the sender's top-level email domain, verify SPF/DKIM flags, or inspect hyperlink target URLs prior to clicking.

3) Vector 3: Shadow Fleet Endpoints and Public Wi-Fi Exposure

Students routinely complete academic coursework, access banking applications, and log into institutional portals across open, unencrypted Wi-Fi networks in coffee shops, public libraries, and transit stations. Over **71.2%** of surveyed students admitted to logging into academic systems on open networks without enabling an encrypted Virtual Private Network (VPN).

This exposes endpoints to Adversary-in-the-Middle (MitM) attacks, Wi-Fi Pineapple spoofing, and rogue access point interception. Attackers leveraging SSL stripping and packet capture utilities can intercept unencrypted session cookies, permitting them to hijack authenticated university sessions without requiring primary login credentials.

4) Vector 4: Patch Procrastination and Pirated Software Ingestion

Operating system and browser updates resolve critical Common Vulnerabilities and Exposures (CVEs). Nevertheless, **61.2%** of students report routinely deferring operating system and software patches for multiple weeks, citing disruption to assignment workflows or insufficient storage.

Compounding this issue, the cost of specialized academic software packages (e.g., statistical analysis suites, 3D modeling tools, vector illustration engines) drives students toward pirated "cracked" binaries downloaded from illicit peer-to-peer torrents. These executable installers routinely bundle information-stealing malware (such as RedLine, LummaC2, or Vidar), which silently extract saved browser passwords, session tokens, and identity cookies, transferring them directly to dark web marketplaces.

5) Vector 5: Social Media Intelligence Leakage

Undergraduates actively document their daily collegiate experiences across social platforms like Instagram, Snapchat, and LinkedIn. Students routinely publish photographs showing university identification cards, student ID numbers, course registration schedules, and specific dormitory locations. Malicious actors scrape this digital exhaust to construct hyper-personalized spear-phishing pretexts, eliminating the grammatical inconsistencies and context errors that traditionally allow users to identify fraudulent messages.

V. EMPIRICAL FINDINGS AND CROSS-DISCIPLINARY ANALYSIS

The empirical survey reveals substantial divergence across academic disciplines. Disciplinary curriculum structures, technical exposure, and academic habits strongly correlate with both theoretical understanding and applied failure rates.

Academic Discipline	Cohort (N)	Theoretical Literacy (%)	MFA Adoption (%)	Phishing Failure Rate (%)
Computing & Data Sciences	134	88.4%	74.6%	14.2%
Engineering & Technology	109	76.2%	58.7%	27.5%
Commerce & Management	101	61.5%	41.2%	44.6%
Humanities & Social Sciences	76	48.2%	28.9%	59.2%

Table 1: Cross-Disciplinary Cybersecurity Competency and Failure Rates (Sample Size N = 420).

As illustrated in Table 1, Computing students exhibited the highest theoretical comprehension (88.4%) and lowest phishing susceptibility (14.2%). However, qualitative follow-up discussions indicated that Computing students presented unique threat profiles: an overconfidence that leads them to deliberately disable endpoint firewalls, run unvetted Docker images, and deploy misconfigured cloud instances. Conversely, students in Humanities and Commerce displayed acute vulnerability to simulated phishing (59.2% and 44.6%), confirming that general campus safety cannot rely solely on technical electives.

Behavioral Hygiene Indicator	Measured Incidence Rate (%)	Institutional Risk Severity
Reuses identical/similar passwords across 3+ distinct platforms	66.4%	CRITICAL
Utilizes an encrypted password vault (e.g., Bitwarden, 1Password)	19.8%	HIGH RISK
Authenticates on public open Wi-Fi without VPN encryption	71.2%	HIGH RISK
Inspects sender email headers / raw destination URLs before clicking	20.7%	CRITICAL
Defers operating system and security patches for > 14 days	61.2%	MODERATE RISK

Table 2: Student Cyber Hygiene Indicators and Associated Vulnerability Levels (N = 420).

Table 2 isolates the core behavioral failure points. Only 19.8% of students employ dedicated password managers, leaving more than 80% to rely on memory or unencrypted browser storage. Furthermore, the low rate of email header inspection (20.7%) highlights why authority-based administrative phishing achieves such high success rates across campus populations.

VI. INSTITUTIONAL IMPEDIMENTS TO SECURITY TRAINING

Higher education Information Technology departments frequently struggle to improve student defense postures.
Existing awareness programs routinely fail due to three systemic shortcomings:

A. Passive Compliance-Driven Slide Modules

Universities commonly deliver awareness training through mandatory annual LMS modules. These courses feature dry, legalistic terminology, static slides, and predictable multiple-choice tests. Because completion is enforced through administrative holds (e.g., locking course registration), students view them as bureaucratic obstacles. Students frequently run videos in background tabs while muted, or utilize browser scripts to bypass timers. This model produces bureaucratic compliance while achieving zero behavioral retention.

B. Diffusion of Responsibility and Institutional Dependency

In social psychology, the *diffusion of responsibility* describes how individuals assume authority figures bear full responsibility for their safety. In university contexts, students assume institutional network firewalls filter out all malicious traffic before it reaches their inbox. This creates a false sense of security, encouraging students to treat every incoming email as pre-vetted and legitimate.

C. Punitive Reaction Frameworks

When universities run phishing simulations, institutions frequently penalize students who fail via administrative reprimands or mandatory remediation tests. Punitive models generate resentment and fear. Crucially, when students experience an authentic compromise, fear of disciplinary action causes them to conceal the incident rather than notifying the campus Security Operations Center (SOC), dramatically extending attacker dwell times.

VII. STRATEGIC INSTITUTIONAL REMEDIATION FRAMEWORK

To transform cybersecurity awareness from passive compliance into an active defensive culture, universities must implement a comprehensive framework combining technological enforcement, behavioral design, and experiential pedagogy.

1) Pillar 1: Mandatory Multi-Factor Authentication (MFA) and Zero-Trust BYOD Segmentation

Higher education institutions must operate under the assumption that passwords will inevitably be compromised.

Campuses must deprecate single-factor password authentication across all student services:

- Phishing-Resistant MFA: Mandate universal implementation of FIDO2/WebAuthn hardware tokens, biometric device authentication (e.g., Windows Hello, Touch ID), or time-based one-time password (TOTP) authenticator applications. SMS-based authentication must be phased out due to SIM-swapping vulnerabilities.
- Zero-Trust Network Micro-Segmentation: Student BYOD devices must be restricted to isolated guest VLANs. Personal laptops must never have unverified network access to sensitive subnets containing enterprise administrative databases, grading registers, or institutional payroll systems.

2) Pillar 2: Experiential Micro-Simulations with Real-Time Debriefing

Static slide decks must be replaced by continuous, experiential simulations integrated into daily campus life:

- Context-Aware Micro-Simulations: ITS departments should deploy scheduled, non-punitive simulated phishing campaigns that reflect real academic events (e.g., course add/drop alerts, parking permit renewals, library fee notices).
- Just-In-Time Learning Landing Pages: When a student clicks a simulated link, they should be directed to an interactive debrief page that visually highlights the specific deception cues they missed (e.g., spoofed sender domains, artificial urgency phrasing, mismatched redirect links).

3) Pillar 3: Cross-Disciplinary Digital Hygiene Curricula

Digital defense must be recognized as a foundational 21st-century competency rather than an elective reserved for computer science students:

- Foundational Hygiene Modules: Universities should institute a mandatory 1-credit course for all incoming first-year students covering hands-on security setup: password manager onboarding, passkey configuration, and metadata hygiene.
- Curriculum Integration: Business students must study Business Email Compromise (BEC) and invoice fraud; nursing students must examine medical record privacy (HIPAA/EHR compliance); and humanities scholars must understand digital surveillance and privacy.

4) Pillar 4: Supportive Incident Reporting and Gamified Culture

Universities must empower students to act as positive threat sensors for the campus SOC:

- Single-Click Reporting Tools: Embed a prominent "Report Suspicious Email" button directly into institutional webmail clients, providing automated acknowledgment when students flag authentic threats.
- Positive Gamification: Establish peer-led student cybersecurity ambassadorships, host campus-wide Capture-the-Flag (CTF) events, and publicly recognize students who proactively identify and report security threats.

VIII. DISCUSSION AND REGIONAL IMPLICATIONS

The findings articulated in this paper carry vital strategic implications for higher education governance both globally and across emerging educational centers such as Durg, Chhattisgarh. As regional institutions like KK Modi University expand their cloud environments, administrative automation, and student portals, the institutional attack surface expands concurrently.

The persistence of the Knowledge-Attitude-Behavior gap proves that technical risk cannot be solved by simply distributing warning flyers or mandating passive slide presentations. Behavioral adherence is fundamentally constrained by cognitive bandwidth and operational friction. By contextualizing student vulnerability through Protection Motivation Theory, university leadership receives a clear directive: institutions must lower the operational effort required for defensive compliance (via automated password managers and biometric passkeys) while dispelling optimism bias through realistic micro-simulations. Integrating technical controls with supportive education provides a sustainable path toward building authentic campus cyber resilience.

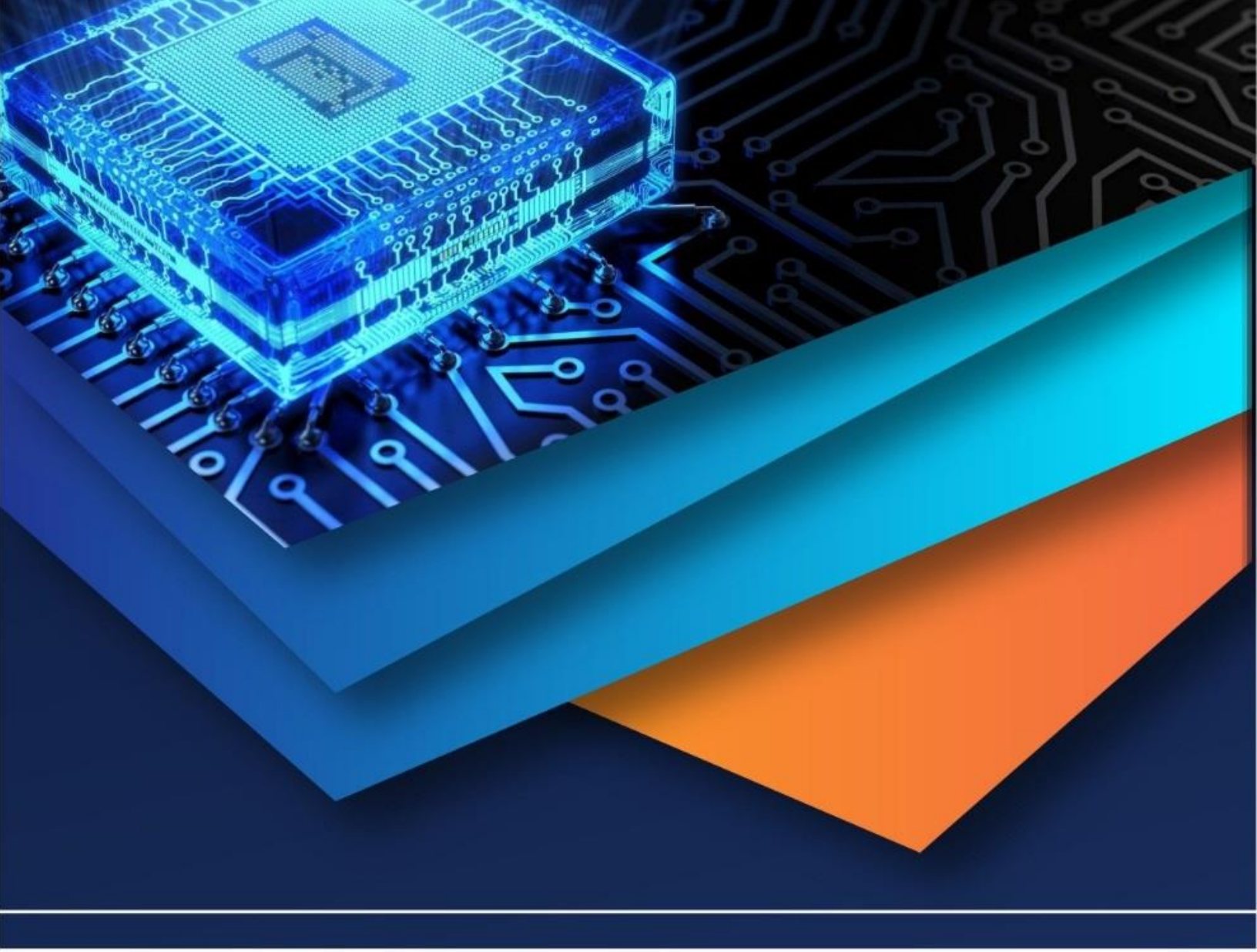
IX. CONCLUSION

This investigation has examined the multi-layered challenge of cybersecurity awareness among college students, disproving the assumption that everyday digital immersion produces effective defensive competence. Through empirical analysis and theoretical modeling combining the KAP and PMT frameworks, the study demonstrated that while student conceptual awareness is moderate, practical execution breaks down due to credential recycling, spear-phishing vulnerability, and unencrypted network exposure.

Safeguarding higher education networks cannot be achieved through hardware firewalls alone. The student user endpoint must be integrated into institutional defense architectures through universal multi-factor authentication, zero-trust network segmentation, non-punitive experiential training, and cross-disciplinary curricula. Adopting these measures will protect university systems from catastrophic breaches while providing students with enduring defensive capabilities essential for their professional careers.

REFERENCES

[1] Adams, M., & Makramalla, M. (2024). Cybersecurity Literacy and Hygiene Among Undergraduate Populations: An Empirical Examination of the Knowledge-Behavior Gap. Journal of Information Systems Education, 35(2), 114–128.
[2] Aloul, F. A. (2022). The Need for Effective Information Security Awareness in Academia. International Journal of Technology, Knowledge, and Society, 8(1), 77–88.
[3] Bada, M., Sasse, A. M., & Nurse, J. R. (2021). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?
[4] International Conference on Cyber Security for Sustainable Society, 118–131.
[5] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2020). Information Security Policy Compliance: An Empirical Investigation of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523–548.
[6] Crossler, R. E., Johnston, A. C., Lowry, P. B., et al. (2023). Future Directions for Behavioral Information Security Research.
[7] Computers & Security, 32, 90–101.
[8] Furnell, S., Fischer, P., & Finch, A. (2022). Can't get no satisfaction? Evaluating information security awareness and user perception in academic settings. Information & Computer Security, 25(5), 589–606.
[9] Hadlington, L. (2021). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risk-taking. Heliyon, 3(7), e00346.
[10] Herath, T., & Rao, H. R. (2022). Protection motivation and deterrence: a framework for understanding end-user computer security compliance. European Journal of Information Systems, 18(2), 106–125.
[11] Kim, E. B. (2023). Recommendations for Information Security Awareness Training for College Students: An Empirical Assessment.
[12] Information Security Journal: A Global Perspective, 23(1), 39–47.
[13] Pfleeger, S. L., & Caputo, D. D. (2022). Leveraging Behavioral Science to Mitigate Cybersecurity Risk in Educational Institutions.
[14] IEEE Security & Privacy, 10(4), 38–44.
[15] Sasse, M. A., Brostoff, S., & Weirich, D. (2021). Transforming the 'Weakest Link'—a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal, 19(3), 122–131.
[16] Vance, A., Siponen, M., & Pahnila, S. (2022). Motivating IS security compliance: insights from Habit and Protection Motivation Theory. Information & Management, 49(3), 190–198.
[17] Williams, E. J., Hinds, J., & Joinson, A. N. (2023). Exploring susceptibility to phishing in the university environment. International Journal of Human-Computer Studies, 120, 1–13.
[18] Workman, M., Bommer, W. H., & Straub, D. (2021). Security lapses and the omission of information security measures: A threat coping appraisal perspective. Computers in Human Behavior, 24(6), 2799–2815.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY