International Journal Software Engineering and Computer Science (IJSECS)
6 (3), 2026, 868-878
Published Online December 2026 in IJSECS (http://www.journal.lembagakita.com/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v6i3.8075.

RESEARCH ARTICLE Open Access

A Study of Cybersecurity Awareness among University Information and Communication Technology Staff in Kabul

Abdul Hameed Himat [1*], **Sayed Elham Sadat** [2], **Mohammad Kabir Ahmadi** [3]

[1*] Computer Education Department, Kabul Education University, Kabul, Afghanistan.
[2,3] Department of Information Technology Department, Kabul Education University, Kabul, Afghanistan.

Article History:

Received: July 19, 2026.
Revised: August 6, 2026.
Accepted: August 27, 2026.
Available online: September 20, 2026.
Published: December 1, 2026.

***Corresponding Author:**
hameedhimmat@gmail.com.

Abstract: This study evaluated cybersecurity awareness among ICT staff in universities in Kabul, Afghanistan, and examined whether awareness differed by demographic and professional factors. A quantitative descriptive survey design was employed, with data collected from 36 employees across 10 universities using a structured questionnaire distributed via Google Forms. Analysis in SPSS included descriptive statistics, the Kruskal–Wallis test, and the Mann–Whitney U test. Results indicated a moderate level of cybersecurity awareness overall. The highest mean score was reported for recognizing the importance of protecting sensitive data (M = 3.97, SD = 0.941), whereas the lowest was for effective communication of cybersecurity policies (M = 3.25, SD = 1.052). Inferential tests revealed no statistically significant differences in awareness across age ($H(3)$ = 1.742, p = 0.628), education ($H(2)$ = 0.399, p = 0.819), or work experience ($H(3)$ = 4.826, p = 0.185). Similarly, no significant difference was observed between staff with and without prior cybersecurity training (U = 117.00, p = 0.379). These findings suggest that demographic and professional characteristics do not substantially influence cybersecurity awareness among the respondents. Universities should therefore prioritize strengthening institutional communication of cybersecurity policies and establishing continuous, structured awareness programs to enhance organizational cyber resilience and equip ICT staff to safeguard institutional data.

Keywords: Cybersecurity Awareness; Cybersecurity Training; Quantitative Assessment; ICT Employees; Cyber Resilience.

1. Introduction

The rapid digital transformation of higher education has significantly increased universities' dependence on information and communication technologies (ICT) to support teaching, learning, research, and administrative activities. Digital platforms, cloud computing, institutional databases, learning management systems, and online communication tools have become essential components of modern universities. While these technologies improve operational efficiency and expand access to educational resources, they also expose higher education institutions to a growing range of cybersecurity threats, including phishing, ransomware, malware, social engineering attacks, and unauthorized access to sensitive information (Alrobaian *et al.*, 2023; Ramamurthy & Aquino, 2025).

Cybersecurity has therefore become a strategic priority for universities worldwide. Although institutions invest in technological safeguards such as firewalls, antivirus software, intrusion detection systems, and access control mechanisms, technical measures alone cannot guarantee effective protection against cyber threats. Human-related factors remain one of the leading causes of cybersecurity incidents. Employees who lack adequate cybersecurity awareness may unintentionally compromise institutional security through unsafe password practices, failure to recognize phishing attempts, improper handling of sensitive information, or non-compliance with institutional security policies (Ahmad Badela, 2024; Alharbi & Tassaddiq, 2021). Consequently, cybersecurity awareness is increasingly recognized as a fundamental component of organizational cyber resilience.

Within higher education institutions, ICT staff play a particularly important role in maintaining institutional cybersecurity. Their responsibilities include managing computer networks, administering servers, maintaining information systems, implementing security controls, supporting end users, and protecting institutional data. Because of these responsibilities, ICT personnel are expected to demonstrate a high level of cybersecurity awareness and to model secure computing practices throughout their institutions. However, previous studies indicate that technical expertise does not necessarily translate into comprehensive cybersecurity awareness, particularly regarding emerging cyber threats, institutional security policies, and secure behavioral practices (Helmiawan *et al.*, 2025).

Although cybersecurity awareness has been widely investigated in universities across different countries, most existing studies have focused on students, general university employees, or other categories of technology users. Comparatively little attention has been given to ICT professionals working in higher education institutions, particularly in developing countries where cybersecurity governance and awareness initiatives remain limited. In developing environments such as Kabul, where digital transition is progressing rapidly despite limited resources, cybersecurity training and evaluation practices may be insufficient or inconsistent. Previous studies have highlighted that lack of adequate training, weak organizational support, and limited cybersecurity awareness increase vulnerability to phishing attacks, social engineering, and other cyber threats (Ahme Ismael, 2025; Zwarts *et al.*, 2025). Within Afghanistan, and specifically in Kabul, empirical evidence regarding the cybersecurity awareness of university ICT staff is extremely limited. This lack of localized, data-based research restricts universities' capability to pinpoint awareness divides, promote targeted programs, and boost organizational cyber capacity. A quantitative assessment of cybersecurity understanding among university ICT employees in Kabul is therefore essential to provide empirical evidence for informed decision-making and effective cybersecurity capacity-building programs.

To address this gap, the general objective of this study is to quantitatively assess the level of cybersecurity awareness among university ICT staff in Kabul. Specifically, the study aims to: 1) measure the level of cybersecurity awareness related to common cyber threats, security practices, and data protection among university ICT staff; 2) examine ICT staff awareness of institutional cybersecurity policies and standards; and 3) determine whether cybersecurity awareness levels differ according to demographic and professional characteristics, including age, education, work experience, and prior cybersecurity training. In alignment with these objectives, the research addresses three central questions regarding what the level of cybersecurity awareness is among university ICT staff in Kabul, to what extent these staff members are aware of institutional cybersecurity policies and standards, and whether there is a significant relationship between demographic factors and their level of cybersecurity awareness.

The study offers scientific, practical, and policy implications for higher education institutions in Kabul. Scientifically, it contributes to the growing literature on cybersecurity awareness in higher education by providing empirical data on ICT employees in Kabul universities, thereby establishing a foundation for future research on human security factors in the sector. Practically, the findings provide university managers with valuable data on the strengths and weaknesses of cybersecurity awareness among their ICT personnel. Institutions can utilize these results to design targeted awareness initiatives, enhance the communication of institutional cybersecurity policies, strengthen incident response seminars and workshops, and establish periodic assessments to monitor awareness levels. Furthermore, the findings support institutional leaders and policymakers in formulating standardized cybersecurity awareness strategies, improving cybersecurity

governance, and implementing effective training and policy compliance frameworks, ultimately fostering secure computing behavior and improving institutional cyber resilience across Kabul's higher education sector.

2. Related Work

2.1 Cybersecurity Awareness in Higher Education

Cybersecurity awareness has become an essential component of information security in higher education institutions. Universities increasingly rely on digital technologies for teaching, research, and administrative operations, making them attractive targets for cyberattacks. Previous studies have consistently reported that students, employees, and ICT personnel demonstrate varying levels of cybersecurity awareness regarding password management, phishing detection, secure browsing, and compliance with institutional security policies (Alharbi & Tassaddiq, 2021; Zineddine *et al.*, 2025). Although awareness levels are often reported as moderate to high, these studies indicate that technical knowledge alone does not always translate into secure cybersecurity behavior.

2.2 Human Factors and Secure Cybersecurity Practices

Several studies have emphasized that human behavior remains one of the weakest links in organizational cybersecurity. Research conducted in higher education institutions found that weak password practices, poor understanding of institutional security policies, and limited ability to recognize phishing attacks significantly increase organizational vulnerability (Alrobaian *et al.*, 2023; Ramamurthy & Aquino, 2025). Similarly, Ahmad Badela (2024), Al Zaidy (2025), and Titi (2025) reported that although many users possess basic cybersecurity knowledge, they continue to engage in risky online behaviors, demonstrating a gap between awareness and actual security practices. These findings suggest that awareness programs should focus not only on knowledge acquisition but also on behavioral change.

2.3 Cybersecurity Awareness in Developing Countries

Cybersecurity awareness presents additional challenges in developing countries, where institutions often face limited resources, inadequate training opportunities, and weaker cybersecurity governance. Studies have shown that phishing, vishing, and other forms of social engineering remain effective because users lack sufficient awareness and organizations provide limited cybersecurity support (Ahme Ismael, 2025; Zwarts *et al.*, 2025). These findings highlight the importance of continuous institutional support and awareness initiatives to reduce human-related cybersecurity risks.

2.4 Cybersecurity Training and Organizational Support

The literature also demonstrates that cybersecurity awareness can be improved through structured training and strong organizational commitment. Helmiawan *et al.* (2025) identified knowledge, attitudes, perceived risk, training, and organizational support as key determinants of cybersecurity awareness. Likewise, Korsah (2025) found that institutions with stronger cybersecurity cultures achieved greater cyber resilience. A summary of prior empirical studies examining cybersecurity awareness across educational institutions is presented in Table 1.

Table 1. *Summary of Previous Studies on Cybersecurity Awareness in Higher Education*

Authors (Year)	Country	Research Method	Sample	Key Findings
Abdullahi Ahmed Ismael (2025)	Somalia	Literature Review	Secondary sources	Reported that cybersecurity awareness remains low because of limited cybersecurity education, inadequate institutional policies, and insufficient user training.
Ahmed Al Zaidy (2025)	United States (Florida)	Quantitative Survey	135 university students	Students demonstrated good cybersecurity knowledge; however, many failed to consistently apply secure cybersecurity practices in their daily activities.
Hendrik Zwarts *et al.* (2025)	South Africa	Literature Review and Framework Development	Secondary sources	Proposed a cybersecurity governance maturity model and emphasized continuous awareness training as a critical

				component of organizational cybersecurity.
Khader Musbah Esmail Titi (2025)	Jordan	Mixed Methods	150 university students	Cybersecurity awareness differed according to academic discipline and study location, with IT students exhibiting significantly higher awareness levels.
Muhammad Agreindra Helmiawan *et al.* (2025)	Indonesia	Quantitative (PLS-SEM)	254 users	Cybersecurity training, organizational security culture, and perceived cyber risk significantly influenced cybersecurity awareness.
Norshadila Ahmad Badela (2024)	Malaysia	Quantitative Survey	136 staff and students	Although participants possessed basic cybersecurity knowledge, risky behaviors such as password reuse and opening suspicious emails remained common.
Shouq Alrobaian *et al.* (2023)	Saudi Arabia	Quantitative Survey	739 trainees	Participants showed inadequate cybersecurity awareness, particularly regarding two-factor authentication, firewall usage, and secure online practices.
Talal Alharbi & Asifa Tassaddiq (2021)	Saudi Arabia	Quantitative Survey	576 university students	Students demonstrated insufficient awareness of phishing attacks, malware threats, and secure password management, highlighting the need for cybersecurity education.
Valli Ramamurthy *et al.* (2025)	Papua New Guinea	Mixed Methods	52 employees	Only a small proportion of participants exhibited high cybersecurity awareness, while unsafe internet browsing and poor security practices were widespread.
Abdelhadi Zineddine *et al.* (2025)	Morocco	Quantitative Survey	440 users and webmasters	Participants demonstrated low-to-moderate awareness of HTTPS security, and the study identified frequent SSL/TLS configuration weaknesses that could increase cybersecurity risks.

2.5 Research Gap

Although previous studies have examined cybersecurity awareness among students, employees, and general technology users in different educational settings, limited attention has been given to ICT staff working in universities, particularly in developing countries. Moreover, no empirical study has specifically investigated cybersecurity awareness among university ICT staff in Kabul, Afghanistan. Since ICT personnel are responsible for managing institutional digital infrastructure and implementing cybersecurity controls, understanding their level of awareness is essential for strengthening cybersecurity resilience in higher education institutions. This study addresses this gap by quantitatively assessing cybersecurity awareness among ICT staff across universities in Kabul and examining whether awareness differs according to selected demographic and professional characteristics.

3. Methodology

3.1 Research Design and Participants

This study employed a cross-sectional quantitative survey design to assess cybersecurity awareness among university ICT personnel in Kabul, Afghanistan. A cross-sectional approach was appropriate as it allowed for the standardized measurement of cybersecurity awareness levels and enabled comparisons across demographic and professional groups at a single point in time without intervention. Ethical principles were

strictly observed throughout the research process. Participants were informed about the nature and academic purpose of the study, informed consent was obtained electronically prior to data collection, and participation was entirely voluntary with the explicit right to withdraw at any stage without consequence. Confidentiality and anonymity were ensured by collecting no personally identifiable information. The target population comprised all eligible ICT staff working across 10 universities in Kabul, totaling 40 individuals. Given this small population size (N = 40), a near-census sampling strategy was implemented. A total of 36 valid responses were successfully retrieved from 3 public and 7 private universities, yielding a response rate of 90%. This high response rate minimized sampling error and ensured balanced institutional representation across both public and private higher education institutions within the study context.

3.2 Research Instrument, Validity, and Reliability

The primary data collection instrument was a structured questionnaire developed in direct alignment with the research objectives and questions. The instrument consisted of two main components: the first gathered demographic and background profiles, including age, educational qualification, work experience, university affiliation, and prior cybersecurity training; the second comprised 15 substantive items divided equally into three sections of five items each. These sections evaluated respondents' awareness of common cyber threats and data protection practices, institutional cybersecurity policies and standards, and perceived organizational communication. All substantive items were measured using a standardized five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). To establish content and construct validity, the preliminary questionnaire was evaluated by three university professors specializing in information technology and cybersecurity education. The reviewers examined the clarity, relevance, and alignment of the items with the intended research objectives, and necessary refinements were made based on their evaluations. Instrument reliability was assessed using Cronbach's alpha to determine internal consistency, yielding an overall coefficient of 0.881. Because this value comfortably exceeded the standard benchmark of 0.70, the questionnaire was deemed highly reliable for empirical data collection and statistical testing.

3.3 Data Collection Procedure and Statistical Analysis

Data collection was administered electronically using Google Forms over an approximate 30-day period. The online format facilitated efficient distribution across multiple institutional campuses and provided respondents with adequate time to complete the survey, supported by periodic follow-up reminders. Upon completion of the survey window, all submitted responses were screened for completeness and formatted for statistical analysis. Data were coded and analyzed using IBM SPSS Statistics. Preliminary data screening included descriptive statistics and normality testing. The Shapiro–Wilk test indicated that the awareness scores significantly deviated from a normal distribution ($p < 0.05$). Consequently, nonparametric inferential tests were applied at an alpha level of 0.05. Specifically, the Kruskal–Wallis test was used to examine differences in cybersecurity awareness across categories of age, education, and work experience, while the Mann–Whitney U test was conducted to evaluate differences based on prior cybersecurity training status.

4. Result and Discussion

4.1 Results

The empirical results of this study are based on 36 completed questionnaires retrieved from ICT personnel across 10 universities in Kabul, utilizing Google Forms as the survey administration platform. The data were screened, coded, and analyzed through descriptive and nonparametric inferential procedures, as detailed in the following subsections. The preliminary evaluation examined the personal background of the respondents, focusing specifically on their age profiles and highest educational qualifications. The age distribution indicates that a dominant proportion of the workforce is concentrated in early-to-mid career stages, with 69.4% of respondents aged between 25 and 34 years, 19.4% between 35 and 44 years, and an equal proportion of 5.6% situated below 25 years and between 45 and 54 years, respectively, as detailed in Figure 1. In terms of academic credentials, the sample reflects a well-educated technical cohort, wherein 66.7% hold a bachelor's degree, 25.0% possess a master's degree, and the remaining 8.3% have attained a professional diploma, as shown in Figure 2.

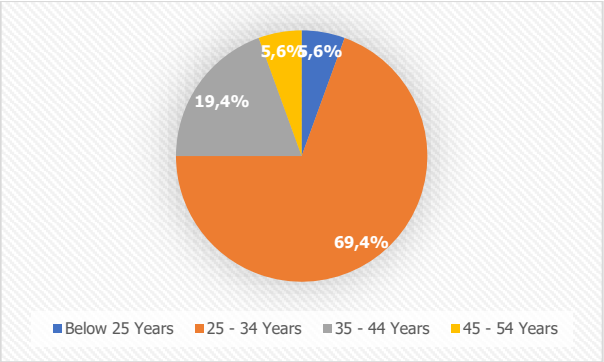

Figure 1. Age Distribution of the Respondents

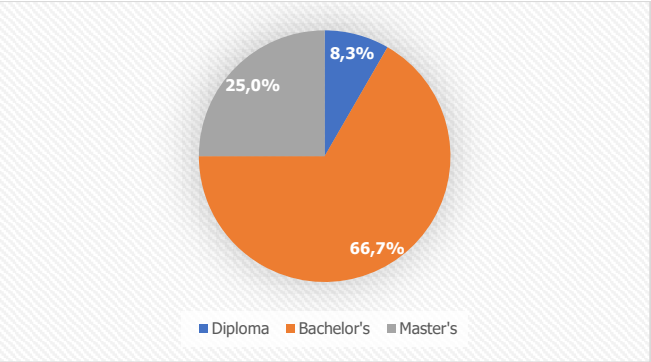

Figure 2. Educational Qualification of the Respondents

Beyond foundational demographics, the survey assessed respondents' professional tenure and their participation in institutional capacity-building programs. Analysis of work history reveals that 61.1% of the personnel possess between 1 and 5 years of professional experience, 13.9% have served between 6 and 10 years, 13.9% have accumulated over a decade in the field, and 11.1% have less than one year of service, as depicted in Figure 3. However, despite their operational roles, a substantial gap exists in formal skill development, with only 33.3% having completed prior cybersecurity training compared to 66.7% who have received no formal instruction, as illustrated in Figure 4.

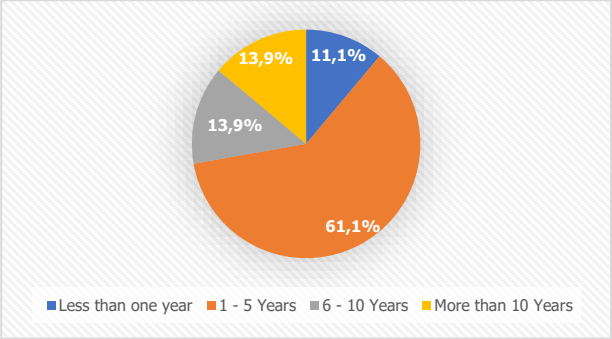

Figure 3. Years of Work Experience of the Respondents

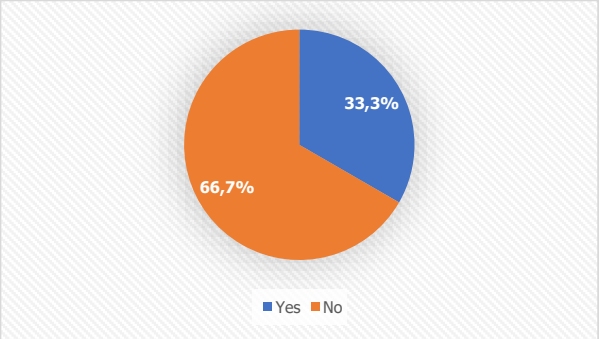

Figure 4. Prior Cybersecurity Training Status of the Respondents

To address the first research objective, participants evaluated their familiarity with common cyber threats, secure communication practices, and sensitive data protection. As summarized in Table 2 and visualized in Figure 5, the mean score for familiarity with common cyber threats was 3.69 (*SD* = 1.261), the ability to recognize suspicious emails and links was 3.75 (*SD* = 1.025), and understanding the safe use of email and computing devices scored 3.78 (*SD* = 1.045). Awareness of best practices against unauthorized system access yielded a mean of 3.83 (*SD* = 0.878), while understanding the importance of protecting sensitive data achieved the highest mean of 3.97 (*SD* = 0.941). These descriptive indices demonstrate an overall moderate level of cybersecurity awareness among university ICT personnel regarding technical safeguards and data protection protocols.

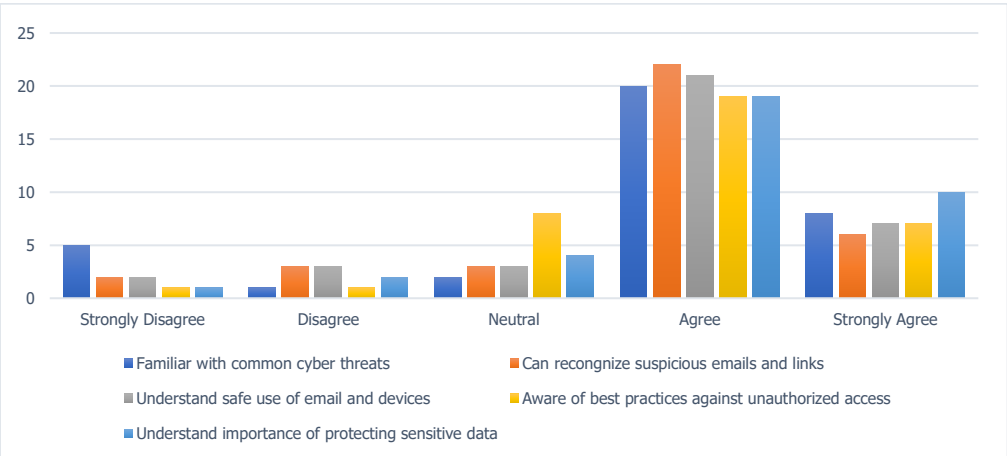

Figure 5. Survey Responses on Cybersecurity Awareness and Practices

Table 2. Respondents' Awareness Level Regarding Common Cybersecurity Practices

Description	Mean	Standard Deviation
Familiar with common cyber threats	3.69	1.261
Can recognize suspicious emails and links	3.75	1.025
Understand safe use of email and devices	3.78	1.045
Aware of best practices against unauthorized access	3.83	0.878
Understand importance of protecting sensitive data	3.97	0.941

To address the second research objective, respondents answered items concerning institutional governance, policy comprehension, data handling standards, and incident response procedures. As presented in Table 3 and depicted in Figure 6, general awareness of university cybersecurity policies yielded a mean of 3.28 (*SD* = 1.085), whereas understanding key policy requirements recorded a mean of 3.33 (*SD* = 1.014). Familiarity with system access and data usage regulations scored slightly higher at 3.67 (*SD* = 0.926). Respondents reported a mean of 3.58 (*SD* = 1.025) regarding knowledge of required actions during a cybersecurity incident. Perceptions regarding whether the university effectively communicates cybersecurity policies recorded the lowest score across all dimensions, with a mean of 3.25 (*SD* = 1.052). These findings indicate that while operational access rules are moderately understood, formal institutional policy communication remains an area requiring substantial reinforcement.

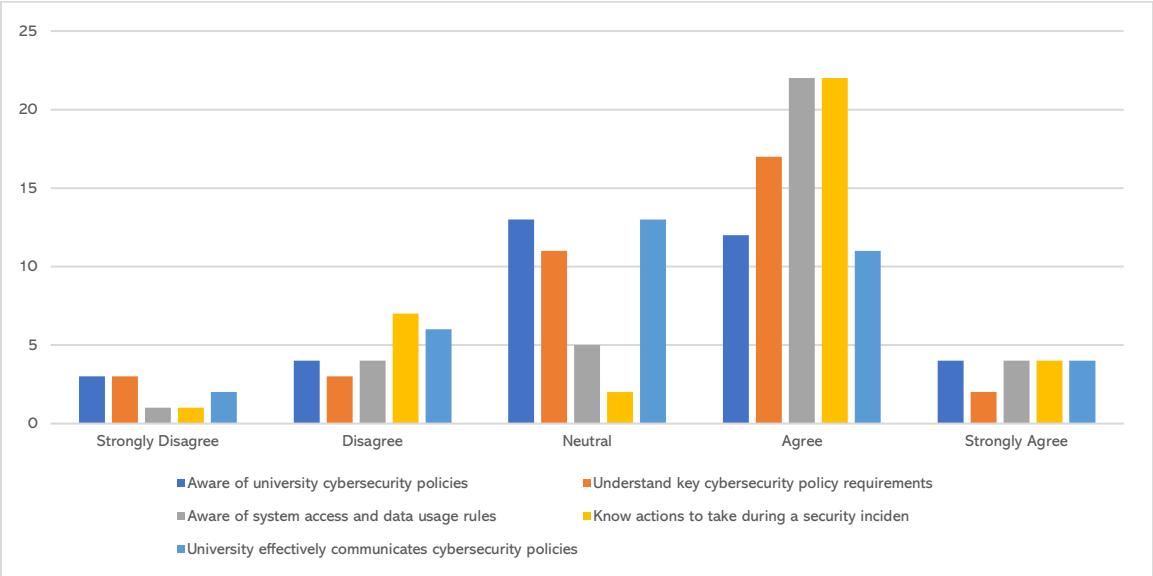

Figure 6. ICT Staff Awareness of Institutional Cybersecurity Policies and Standards

Table 3. Respondents' Awareness Pertinent to Cybersecurity Policies and Standards

Description	Mean	Standard Deviation
Aware of university cybersecurity policies	3.28	1.085
Understand key cybersecurity policy requirements	3.33	1.014
Aware of system access and data usage rules	3.67	0.926
Know actions to take during a security incident	3.58	1.025
University effectively communicates cybersecurity policies	3.25	1.052

To address the third research objective, nonparametric inferential analyses were performed to determine whether cybersecurity awareness differed significantly across demographic and professional categories, with results summarized in Table 4. A Kruskal–Wallis test revealed no statistically significant differences in cybersecurity awareness across age cohorts, $H(3) = 1.742$, $p = 0.628$. Similarly, awareness did not differ significantly across educational qualification levels (diploma, bachelor's, and master's degrees), $H(2) = 0.399$, $p = 0.819$. A third Kruskal–Wallis test evaluated differences across work experience groups and likewise yielded no statistically significant difference, $H(3) = 4.826$, $p = 0.185$. Finally, a Mann–Whitney U test was performed to compare staff who had received prior cybersecurity training against those who had not. The test indicated no statistically significant difference between the two groups, $U = 117.00$, $Z = -0.908$, $p = 0.379$. Collectively, these inferential findings demonstrate that cybersecurity awareness among university ICT personnel in Kabul remains uniform across age, education, professional tenure, and prior training status.

Table 4. Nonparametric Tests for Differences in Cybersecurity Awareness Across Demographic and Professional Factors

Variable	Statistical Test	Test Statistic	df	p-value	Decision
Age	Kruskal–Wallis	$H = 1.742$	3	0.628	Not significant
Education	Kruskal–Wallis	$H = 0.399$	2	0.819	Not significant
Experience	Kruskal–Wallis	$H = 4.826$	3	0.185	Not significant
Training	Mann–Whitney *U*	$U = 117.00$ ($Z = -0.908$)	—	0.379	Not significant

4.2 Discussion

This study evaluated cybersecurity awareness among university ICT staff in Kabul within an institutional setting marked by rapid digital adoption and resource-constrained security infrastructure. The empirical findings indicate that university ICT staff demonstrate an overall moderate level of cybersecurity awareness regarding common cyber threats, secure practices, and sensitive data protection. Respondents exhibited their highest awareness in recognizing the importance of protecting sensitive data ($M = 3.97$) and implementing safeguards against unauthorized access ($M = 3.83$). These observations align with prior scholarship indicating that technical personnel generally maintain sound fundamental knowledge of baseline security measures and data preservation principles (Alharbi & Tassaddiq, 2021; Zineddine *et al.*, 2025). Given that ICT staff administer mission-critical digital systems, this baseline knowledge provides an essential operational foundation for safeguarding higher education networks.

Nevertheless, the comparatively elevated standard deviation observed for familiarity with common cyber threats ($SD = 1.261$) reflects substantial variability in awareness across individual personnel. This divergence corroborates earlier research emphasizing that cybersecurity awareness is rarely homogeneous, even among technical workforces (Alrobaian *et al.*, 2023; Ramamurthy & Aquino, 2025). Such uneven capability represents a vulnerability because organizational systems are frequently compromised through the least security-conscious employees. Consequently, institutional administrators cannot assume uniform security competence across their technical teams solely based on functional job titles.

Regarding institutional cybersecurity governance, respondents exhibited moderate awareness across all policy dimensions, with notable disparity between operational familiarity and organizational communication. While awareness of system access and data usage regulations scored moderately high ($M = 3.67$), the perceived effectiveness of institutional policy communication received the lowest score across the entire survey ($M = 3.25$). This discrepancy indicates that although technical personnel are familiar with routine system protocols, higher-level cybersecurity policies are insufficiently disseminated across universities. These findings echo prior literature highlighting organizational communication and policy clarity as indispensable components of effective cybersecurity governance (Akere, 2024; Helmiawan *et al.*, 2025). Furthermore, respondents demonstrated only moderate confidence regarding incident response protocols ($M = 3.58$), reflecting uncertainty in operationalizing procedural countermeasures when a security breach occurs. Consistent with the behavioral gaps identified by Ahmad Badela (2024), Alzaidi (2025), and Titi (2025), cognitive knowledge of cybersecurity principles does not automatically translate into procedural preparedness during live security incidents.

The inferential analyses revealed that cybersecurity awareness did not differ significantly based on age, educational qualification, work experience, or prior training. The absence of variation across educational levels supports previous conclusions that formal academic degrees do not inherently confer heightened cybersecurity consciousness. Similarly, years of professional tenure do not necessarily enhance threat awareness unless accompanied by regular engagement with modern cyber attack vectors and specialized development programs. Prior participation in cybersecurity training was not associated with significantly higher awareness scores. This finding raises fundamental concerns regarding the curriculum design, duration, and practical relevance of training initiatives accessible to university personnel in Kabul. As documented in previous studies, occasional theoretical instruction is substantially less effective than continuous, hands-on, and scenario-based simulations that cultivate secure behavioral habits (Korsah, 2025; Yangchen, 2025). The absence of a training effect in this study strongly suggests that existing professional development efforts may be irregular, overly abstract, or insufficient to produce durable improvements in threat detection.

These empirical realities offer direct practical implications for higher education institutions in Kabul. In resource-constrained environments, universities can deploy low-cost, high-frequency awareness initiatives without substantial budgetary investments. Actionable interventions include distributing concise weekly security bulletins via institutional email or messaging platforms to reinforce vigilance against phishing schemes, credential compromise, and unverified software downloads. Furthermore, departments can embed 15- to 20-minute briefing segments into regular monthly staff meetings to review emerging threat patterns and institutional response protocols. Periodic benign phishing simulations can also provide safe experiential learning opportunities to reinforce threat detection skills, complemented by digital posters and bulletin boards that clarify incident reporting channels. The methodological context warrants consideration when evaluating

these outcomes. While obtaining 36 valid responses from a total population of 40 represents a robust 90% sampling coverage that minimizes local selection bias, the absolute sample size constrains statistical power and reduces the sensitivity of inferential tests to detect subtle group variations. Consequently, nonsignificant results should not be viewed as definitive proof that demographic factors never influence security behavior. Moreover, as the study sampled staff exclusively within Kabul, generalizability to universities in other Afghan provinces requires caution. Future investigations engaging wider cohorts across diverse geographic regions will further clarify the systemic determinants of cybersecurity awareness in higher education.

5. Conclusion and Recommendations

This study evaluated cybersecurity awareness among university ICT personnel in Kabul, addressing a critical empirical void within higher education institutions operating in developing and resource-constrained environments. As universities accelerate their reliance on enterprise networks, administrative databases, and online academic platforms, examining the human dimension of cybersecurity becomes essential for safeguarding institutional assets. The empirical findings reveal that ICT staff maintain an overall moderate level of cybersecurity awareness, with stronger competence demonstrated in sensitive data protection, authorized system access, and safe computing practices. However, observable variability across responses highlights that awareness is not uniformly distributed throughout technical teams, leaving specific personnel vulnerable to emerging social engineering tactics and sophisticated threat vectors. Awareness of institutional cybersecurity policies and governance frameworks was also moderate, with respondents reporting comparatively lower scores regarding the effectiveness of institutional policy communication. This outcome reveals an organizational disconnect, where operational familiarity with routine access rules is not matched by structured institutional dissemination or policy reinforcement. Furthermore, inferential analyses established that cybersecurity awareness did not differ significantly based on age, educational qualification, professional tenure, or prior participation in cybersecurity training. Notably, the absence of a training effect indicates that existing professional development programs within Kabul universities may be irregular, theoretical, or insufficient to produce durable behavioral improvements. Strengthening institutional cyber resilience therefore requires universities to move beyond ad hoc technical safeguards and institute continuous, behavior-centered awareness frameworks supported by active administrative commitment and clear policy communication.

Several methodological limitations should be considered when interpreting the conclusions of this investigation. Although the obtained sample (n = 36) accounted for approximately 90% of the eligible ICT staff population across the 10 selected universities, the absolute sample size remains modest. This near-census approach provides high internal representativeness within the participating institutions, yet the restricted sample size diminishes statistical power and limits the sensitivity of nonparametric tests to detect subtle group variations across demographic subsets. In addition, because data collection was confined exclusively to higher education institutions in Kabul, caution must be exercised when generalizing these findings to provincial universities or different institutional sectors across Afghanistan. Measurement and temporal constraints also characterize the study design. Reliance on a self-administered questionnaire introduces the possibility of response bias, including social desirability tendencies where respondents may overestimate their procedural compliance or threat knowledge. Consequently, self-reported awareness may not fully reflect operational behavior during active security incidents. Methodologically, the cross-sectional survey captured perceptions at a single point in time, precluding evaluation of longitudinal awareness trajectories or the long-term impact of specific institutional interventions. Furthermore, the inquiry focused exclusively on dedicated ICT professionals, omitting other critical institutional stakeholders such as faculty members, administrative staff, and students. Finally, while nonparametric analyses were appropriately utilized to address non-normal data distributions, effect size metrics were not computed, which could have provided deeper perspective on the magnitude of demographic comparisons.

To address the awareness gaps identified among university ICT personnel in Kabul, higher education administrations and policymakers should pursue targeted institutional reforms. Universities should transition from occasional seminars toward institutionalizing structured, continuous awareness programs. Because technical personnel exhibited uneven threat familiarity, standardized training curricula should be integrated directly into annual professional development requirements. To ensure practical efficacy, instructional design must shift away from abstract theory toward experiential, scenario-based learning models. Implementing controlled phishing drills, simulated breach responses, and hands-on vulnerability workshops will enable personnel to bridge the gap between conceptual understanding and secure operational habits. Simultaneously, institutional leadership must prioritize the communication and accessibility of cybersecurity policies. University administrators should ensure that information security governance documents are regularly updated, simplified into actionable guidelines, and actively disseminated through digital bulletins, briefing sessions, and staff portals. Establishing a robust organizational security culture also demands visible administrative backing,

where leadership allocates dedicated resources, enforces clear accountability mechanisms, and positions cybersecurity as a shared institutional responsibility rather than solely an IT concern. Complementing these initiatives, universities should introduce routine diagnostic assessments to track awareness trends, pinpoint emergent vulnerabilities, and guide data-driven enhancements to their institutional security strategies.

References

Ahmad Badela, N. (2024). Fostering cybersecurity consciousness: Assessing awareness among students and staff in a technical institution. *International Journal of Modern Trends in Social Sciences*, *7*(27), 26–39. https://doi.org/10.35631/ijmtss.727003

Ismael, A. A. (2025). *The lack of cybersecurity awareness in Somalia*. ResearchGate. https://doi.org/10.13140/RG.2.2.31157.38882.

Akere, O. M. (2024). Assessment of internet safety, cybersecurity awareness and risks in technology environment among college students. *American Journal of Multidisciplinary Research and Innovation*, *3*(6), 25–29. https://doi.org/10.54536/ajmri.v3i6.3012

Al Zaidy, A. (2025). Measuring cybersecurity awareness of students: A study of state college students. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence*, *2*(3), 17–40. https://doi.org/10.70715/jitcai.2025.v2.i3.030

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), Article 23. https://doi.org/10.3390/bdcc5020023

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing*, *7*(2), Article 73. https://doi.org/10.3390/bdcc7020073

Alzaidi, N. (2025). Cybersecurity awareness among female students at Taif University's faculty of computing and information technology. *Global Journal of Information Technology: Emerging Technologies*, *15*(1), 47–63. https://doi.org/10.18844/gjit.v15i1.9722

Cheong Tian Ming, R., Rahaman, N. H., Saidi, L. A., Wan Yusof, W. S. E. Y., & Ramlee, S. N. S. (2025). Knowledge, attitude, and password practices: Determinants of cybersecurity awareness among students in Malaysian public universities. *International Journal of Education, Psychology and Counseling*, *10*(59), 1002–1008. https://doi.org/10.35631/ijepc.1059072

Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering*, *12*(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584

Helmiawan, M. A., Firmansyah, E., Herdiana, D., Akbar, Y. H., Subiyakto, A., & Rahman, T. K. A. (2025). Quantitative analysis of the key factors driving cybersecurity awareness among information systems users. *Jurnal Teknik Informatika (JUTIF)*, *6*(4), 1897–1910. https://doi.org/10.52436/1.jutif.2025.6.4.4861

Korsah, D. P. (2025). Evaluating the impact of staff cybersecurity culture on cyber resilience in colleges of education: Insights from 12 colleges of education in Ghana. *Journal of Education and Learning Technology*, *6*(4), 203–218. https://doi.org/10.38159/jelt.2025646

Krikelas, I. (2025). Promoting cybersecurity awareness in primary education: A classroom approach to online safety education. *European Journal of Contemporary Education and E-Learning*, *3*(6), 34–44. https://doi.org/10.59324/ejceel.2025.3(6).03

Lim, Y. Z., & Tan, A. J. (2025). Cybersecurity awareness among youth: What's vital? *Paper Asia*, *41*(2), 166–172. https://doi.org/10.59953/paperasia.v41i2b.334

Rama, P., Marx, B., & Smith, R. (2025). Cybersecurity awareness among accounting students at a South African public university. *South African Journal of Information Management*, *27*(1), Article a1948. https://doi.org/10.4102/sajim.v27i1.1948

Ramamurthy, V., & Aquino, E. (2025). Evaluating cybersecurity awareness and practices among employees at a private university in Papua New Guinea. *IBSUniversity Journal of Business and Research*, *2*(1), 1–15.

S., K., & Jegadeeshwaran, M. (2024). Quantitative assessment of the cybersecurity and cybercrime awareness among postgraduate commerce students in the Coimbatore District, India. *Asian Journal of Probability and Statistics*, *26*(9), 185–197. https://doi.org/10.9734/ajpas/2024/v26i9653

Titi, K. M. I. (2025). Comprehensive analysis of cybersecurity awareness among students' universities. *International Journal of Innovative Technology and Exploring Engineering*, *14*(5), 6–14. https://doi.org/10.35940/ijitee.E4613.14050425

Yangchen, T. (2025). Strengthening digital defences: Evaluating the impact of cybersecurity awareness workshops among first-year engineering students in Bhutan. *Bhutan Journal of Research and Development*, *14*(3), Article 8. https://doi.org/10.17102/bjrd.rub.14.3.008

Zineddine, A., Belfaik, Y., Sadqi, Y., & Safi, S. (2025). A novel hybrid cybersecurity assessment methodology for HTTPS deployment. *High-Confidence Computing*, *5*(3), Article 100344. https://doi.org/10.1016/j.hcc.2025.100344

Zwarts, H., Du Toit, J. L., & Von Solms, B. (2025). *Augmenting cybersecurity awareness at critical infrastructures in developing countries through a cybersecurity governance maturity model* [Conference paper]. University of Johannesburg Institutional Repository. https://hdl.handle.net/10210/517571.