Author's name: Zabihullah Nadry. "Strengthening Cybersecurity Awareness Through Education: The Expanding Role of Cyber Law in Academic Institutions" Jurnal Analisis Hukum 8 no. 2 (2025): 193-209.
DOI: https://doi.org/10.38043/jah.v8i2.7086

Jurnal Analisis Hukum
Volume 8 Issue 2, 2025
P-ISSN: 2620-4959, E-ISSN: 2620-3715

Strengthening Cybersecurity Awareness Through Education: The Expanding Role of Cyber Law in Academic Institutions

Zabihullah Nadry [1*], Musawer Hakimi[2], Abdul Wali Sirat[3], Zekrullah Popal[4]

[1]Department of Geography, Education Faculty, Samangan University, Aibak, Afghanistan,
E-mail: zabinadry200@gmail.com
[2]Department of Computer Science, Education Faculty, Samangan University, Samangan, Afghanistan,
Email: Musawer@adc.edu.in
[3]Department of History, Education Faculty, Samangan University, Samangan, Afghanistan,
Email: abdulwalis123@gmail.com
[4]Department of Software Engineering, Computer Science Faculty, Avicenna University, Afghanistan,
Email: Zekrcu@gmail.com

Abstract: As digital technologies continue to proliferate, university students are especially vulnerable to the risks associated with cyber threats, and there is a dearth of research related to the cybersecurity awareness of university students in a developing country context. The purpose of this study is to examine the cybersecurity knowledge, attitudes, and practices of first-year students at Kabul University in Afghanistan to determine the influence of gender, faculty, and awareness of cyber law on intentions to engage in secure online behavior. To collect data, we conducted a cross-sectional survey of 371 students who were recruited using stratified random sampling. Participants were introduced to and administered a survey using the Contextualized Cybersecurity Educational Research Instrument (CCERI), and data was analyzed on SPSS using descriptive statistics, independent samples t-tests, ANOVA, Chi-square tests, and multiple regression models. The results indicated that students had moderate to high levels of cybersecurity knowledge and generally positive attitudes, but that they demonstrated fewer secure practices and a knowledge-practice gap emerged. Male students and students from the Computer Science faculty had greater awareness of cybersecurity and higher recognition of phishing attempts than female students and students from the other faculties. Multiple regression models indicated that cybersecurity knowledge, attitudes, and awareness of the cyber law were significant predictors of secure behavior; this suggests that we need to develop and integrate educational interventions to support positive behaviors in terms of secure cyber practices. Our research adds new knowledge by integrating awareness of cyber law with cybersecurity behavior in Afghanistan as its own unique context. We conclude with recommendations for evidence-informed decisions to implement and develop institutionalized programs to address capacities in cybersecurity education for students in Afghanistan.

Keywords: Cybersecurity Awareness; Cyber Law; Student Behavior; Higher Education; Knowledge-Practice Gap

1. Introduction

The modern era of digitization, cybersecurity awareness in academia has never been more critical not only for the security of institutional resources but also for preparing students to manage increasingly complex online environments. With e-learning platforms, intelligent education systems, and e-communications tools being implemented at a rapid pace, universities and colleges are becoming more vulnerable to cyber-attacks on both technical infrastructure and human aspects. This threat is

especially acute in first-year students who, despite being digital natives, have not received foundational cybersecurity awareness training and are vulnerable to phishing, social engineering, and poor passwords (Ahmad et al., 2021; Al-Fatlawi, 2024).

Universities are incorporating some level of cybersecurity training and cyber law education as part of their holistic resilience approach. Important to note is that national and individual institutional policies also contribute significantly to the student's behavior in the area of cybersecurity. For example, the European Union's General Data Protection Regulation (GDPR) has a high standard to which universities must meet for data privacy, and in doing so also shapes students to behave in better data-handling manner. In the US, for example, laws such as the Family Educational Rights and Privacy Act (FERPA) govern the privacy of student education records and have prompted institutions to implement stronger access controls and authentication procedures, indirectly encouraging a culture of security among students (Ahmad et al., 2021; Al-Fatlawi, 2024).

In addition, universities tend to have acceptable use policies (AUPs) in place and comply with codes of conduct that embody both legal responsibilities and cybersecurity best practices. Violations ranging from inappropriate use to the misappropriation of data could lead to both academic consequences and legal ramifications, which should remind us of our responsibility for our online conduct. There are also cybersecurity training programs that are required as part of compliance obligations (e.g., NIST standards for research universities), in which students are able to learn the legal obligations associated with careers and to practice good security hygiene early on(Khader et al., 2021; Kumar et al., 2024).

Literature has revealed several strategies for improving cybersecurity education. For instance, Al-Janabi and Al-Shourbaji (2016) conducted research on cybersecurity awareness in educational facilities across the Middle East and drew the conclusion that there exists awareness, but its application is imbalanced and not standardized. Similarly, Chang and Coppel (2020) made note of the importance of national policies within developing countries, showing how within non-institutionalized education systems, awareness is disaggregated. Cheng and Wang (2022) and Filipenko et al. (2025) recently proposed institutional response measures and information security policy models for higher education, emphasizing the importance of formalized governance processes. These attempts underscore the diversity of methods but also show a lack of uniform models attuned to different institutional and cultural contexts.

For best practice, evolution in establishing a cybersecurity culture on a university level has been scrutinized to a larger extent.Armas and Taherost (2025) proposed a unified perspective of integrating cybersecurity culture within higher education; and Furnell and Vasileiou (2022) proposed an integrated approach to cyber security education credentials as a way of endorsement in higher education teaching and learning context. Additionally, Shillair et al. (2022, 2023) highlighted the need to have evidence based awareness campaigns at the institutional and national levels, with the support of partnerships, and integration of cross sectoral partnerships, for improvement in training efforts.While these works have value in raising awareness, they emphasize technical training and counseling, somewhat neglecting the legal aspects, namely how a cyber law sets the context and parameter for staff and student awareness.

A noteworthy issue mentioned in the literature is the disconnect between national legal frameworks and educational programming. Alwan (2019) and Shah et al. (2021) treated cybersecurity and legal frameworks as operating at a national level but did not consider how these were interpreted and enforced at the institutional level. The lack of engagement in this discussion is a lost opportunity for educators to consider providing students and employees with legal literacy, especially in the context of cyber law. Legal literacy in cybersecurity courses must be addressed so that a person understands his or her technical function and the legal rights and obligations that exist in a virtual environment.

Cybersecurity legislation such as data protection acts, cybercrime legislation, and consumer protection acts has a substantial impact on educational materials and institutional policies. For example, the General Data Protection Regulation (GDPR) in the EU requires all institutions that handle personal data to implement privacy-by-design, which in turn requires universities to offer specifically targeted training on data treatment, consent, and consequences of breaches. In the US, there are statutes such as the Computer Fraud and Abuse Act (CFAA) and FERPA, which govern unauthorized access and student confidentiality, that require the development of codes of conduct and acceptable uses policies at the institution that are required to be shared and understood by all affected parties, from students to faculty (Shah et al. 2021).

In addition, national cyber security policies frequently contain education mandates, including obligatory awareness modules or summaries of legal advice, meant to reinforce a "security-first" culture. These systems shape how institutions want to integrate proper training methods, build risk assessment frameworks, and adjudge compliance with legislation. Yet, learning programs continue to lack consideration of the legal parameters of cybersecurity, such as obligations through data protection legislation, privacy interests, and liability for negligence or facilitating cybercrime (Khader et al., 2021; Kumar et al., 2024).

The novelty of this study lies in highlighting the gap to be filled between cyber law and cybersecurity awareness education within academic curricula, thereby offering an all-around framework. By integrating legal literacy into the curriculum of cybersecurity, the article aims to equip students not only with technical competencies but also with an understanding of the regulatory and ethical environment that underlies online interactions. This provides the existing technical as well as policy-centered approaches an additional dimension that will make individuals and institutions more resilient.

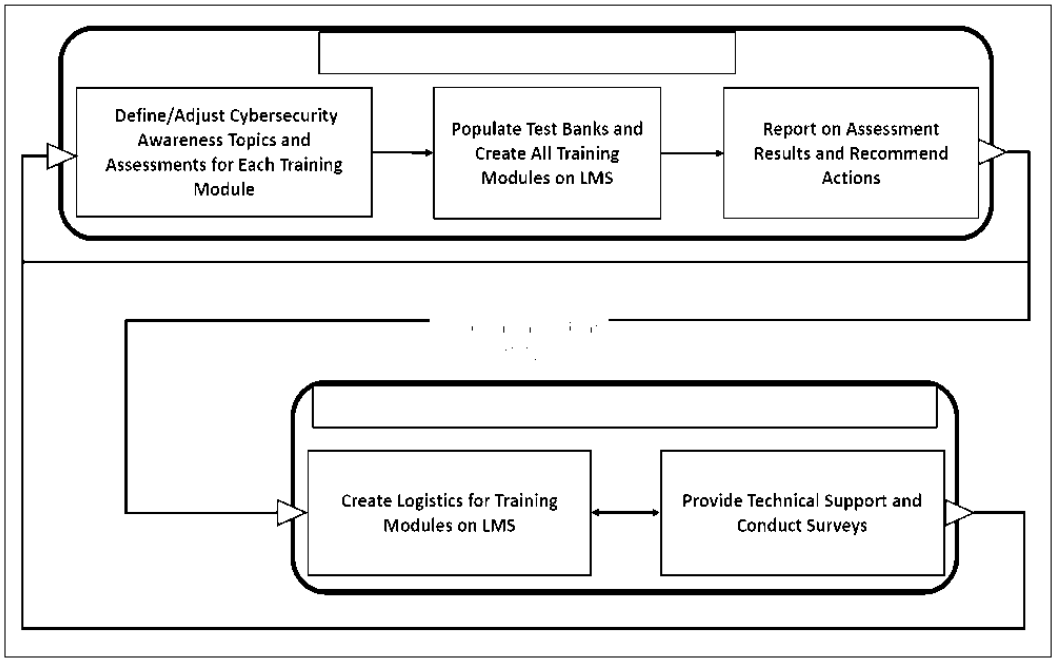

Figure 1. Proposed Cybersecurity Awareness and Support Framework for Higher Education Institutions

The above figure presents a general view of implementing cybersecurity awareness at universities with an orientation towards synchronization of the Cybersecurity Awareness Center (CAC) with Information and Communication Technology Support (ICTS) and the Student Information System (SIS). The CAC identifies and customizes cybersecurity issues, creates training modules in the Learning Management System (LMS), and reports on test outcomes to inform action. Meanwhile, ICTS offers logistical module arrangement, technical support, and effectiveness surveys. The SIS acts as a single-stop repository to enable communication and monitoring of student participation. The system is centered on a planned, institutional approach to enhancing cybersecurity awareness, which makes training routine, clear, and responsive to students. Such a framework corroborates the previous studies in favor of institutional patronage, systematic training, and assessment-based awareness programs as being imperative to developing a cybersecurity-aware population (Ahmad et al., 2021; Al-Fatlawi, 2024; Ali et al., 2025; Al-Janabi & Al-Shourbaji, 2016; Alwan, 2019; Armas & Taherdoost, 2025; Bada & Nurse, 2019; Chang & Coppel, 2020; Cheng & Wang, 2022; Filipenko et al., 2025; Furnell & Vasileiou, 2022).

Implementation of the framework can encourage sustainable cybersecurity culture, increase awareness and safe behavior among students, and provide actionable recommendations to further enhance continually cybersecurity education in higher education institutions.

Consequently, this paper addresses the following primary objective: to address the expanding aspect of cyber law toward bolstering cybersecurity awareness in schools, with regard to the problem of identifying best practices, assessing flaws in existing practices, and proposing an overall awareness paradigm. The newness of this study lies in its contribution to establishing a systematic educational framework that integrates

cybersecurity awareness with legal liability, thus making a more liable and stronger academic community.

2. Method

Research Design

For the current research, quantitative research design has been adopted, and a cross-sectional survey has been employed to study first-year undergraduate students in Kabul University regarding their beliefs and cybersecurity awareness levels. This method enables measuring KAP of knowledge with respect to cybersecurity in a large population within a short period of time. One of the most important aspects of the survey is an attempt to understand how aware students are of cyber law and how such knowledge of the law impacts behavior in cybersecurity.

The questions on cyber laws were made to assess awareness of rights and responsibilities under the law, for example what is at stake for cybercriminals engaging in activities such as data theft or unauthorized access, and what students know about protections regarding data privacy. Such questions are behaviorally related, asking respondents to make legal connections between their online activities, such as password sharing, online consent, or misuse of institutional sites. To expand the legal dimension of the approach, it is conceivable that future inquiries can use scenarios relating to legal questions, testing adherence to organizational policies and practices as well as cross-national examination of national and global laws and policies involving the protection of personal data, thereby illuminating how the concept of legal literacy has legitimate connections to the culture of cybersecurity in schools. This broader consideration would assist in conceptualizing how legal literacy could promote the culture of cybersecurity in schools.

Most importantly, placing legal contexts into the study of cybersecurity is consequential not only legally in developing aware of the situation, but also legally for building more accountable and sustainable digital learning.

Participants

The study population is first year undergraduate students registered at Kabul University for the academic year of study. First-year students are depicted as vulnerable here because it is most likely they would not have had organized exposure to cybersecurity education nearly at on a postgraduate level, while at the same time being participants in an online service provider for learning. Both students who are enrolled in the online/virtual learning programs, as well ground learning, will be included in the study. In order to maintain emphasis on entry-level students, postgraduate students, and visiting students will be excluded.

Sampling Strategy and Sample Size

To ensure representativeness across different academic disciplines, the study employs stratified proportional random sampling. Each faculty (e.g., Computer Science, Engineering, Economics, Education, Law, Humanities, and Social Sciences) is treated as

a stratum. Students are randomly selected within each stratum in proportion to its size in the total first-year population.

The sample size is determined using Yamane's formula with a 95% confidence level and 5% margin of error:

$$n = \frac{N}{1 + Ne^2}$$

Where:

- n = required sample size
- N = population size
- e = margin of error (0.05)

Assuming an estimated first-year student population of **5,000**, the calculation is as follows:

$$n = \frac{5000}{1 + 5000(0.05^2)} = \frac{5000}{1 + 12.5} = \frac{5000}{13.5} \approx 371$$

Thus, the recommended sample size is 371 students, proportionally distributed across faculties. For example, if the Faculty of Computer Science has 800 students (16% of the population), approximately 60 students will be randomly selected from that faculty.

Data Collection Instruments

The information was gathered using a standardized questionnaire and a brief objective test:

Questionnaire: This collects demographic information (age, gender, faculty), beta self-reported cybersecurity behaviors and attitudes towards cyber law and digital security. Items were utilized to establish dimensions of awareness based on best practice (circa assessment of phishing, social engineering, malware protection, and data privacy.

Items were rated on a 5-point Likert-type scale, as described above.

Objective Test: 15-20 multiple-choice questions that assess factual knowledge of cybersecurity principles (e.g., creating effective passwords, recognizing phishing, and staying away from using mobile devices).

Both tools were pilot tested for readability, clarity, and cultural appropriateness among 25 students. Reliability checked through Cronbach's alpha calculations; a .70 alpha accepted to verify reliability. Content validity guaranteed by cybersecurity and education professionals/faculty members from Kabul University, reviewing the items for content accuracy.

Data Collection Process

Data collected in the regular class meeting in designated classrooms and computer labs. Online students receive the same via a secure digital survey by Google Forms or the institutional LMS. Participants provided the same instructions stating anonymity and were asked to complete the survey. Both survey tools' total completion time will be approximately 25-30 minutes per student.

Data Analysis

The data were examined and coded using SPSS.

Descriptive statistics (e.g., frequencies, means, percentages, standard deviations) were used to summarize participants' cybersecurity knowledge, attitudes, and practices.

Inferential statistics include independent sample t-tests and ANOVAs to compare faculty and gender differences in the level of awareness.

Chi-square tests were undertaken for categorical data (e.g., gender and awareness of phishing).

Regression analysis identifies predictors of secure cybersecurity behavior (e.g., does awareness of cyber law influence practice?)

Ethical Considerations

An ethics application was submitted to the Kabul University Institutional Review Board (IRB) for approval. Participation will be voluntary, and informed consent will be obtained before data collection. Participants will be assured of confidentiality and anonymity, and the ability to withdraw at any time. Data will be securely stored and only accessible to the research team, and for academic use only.

3. Result and Discussion

The sample of 371 first-year Kabul University students revealed moderate to high level of cybersecurity awareness and positive beliefs, but unsafe behavior. The awareness was statistically significantly different between gender and faculties, with the male and Computer Science students most aware of cyber security. Legal knowledge, specifically pertaining to national cyber law, was identified as a significant predictor of safe behavior ($\beta = 0.25$, $p = 0.006$). This supports the assertion that incorporating legal literacy into education such as national cybercrime laws, data protection legislation, and procedures related to institutional compliance into educational curricula will lead to better information security. Gender differences, particularly in identifying phishing e-mails and grappling with the issues of legal discernment, further support the notion of a tailored, gendered approach to the legal literacy education for female college students in order to help them identify their rights as well as the legal implications if they encounter imminent online risk. Similarly, students in non-technical schools of study, such as Education and Economics, can benefit from discipline-specific modules putting cyber law into the context of their subjects for example, digital privacy laws in education or protection of financial data. By incorporating legal literacy into faculty curricula and supporting rights-based, inclusive digital safety education, institutions can bridge gaps in cybersecurity behavior and render all students, regardless of gender or academic background, legally informed and behaviorally capable to navigate a complicated cyber environment.

Demographic Characteristics of Respondents

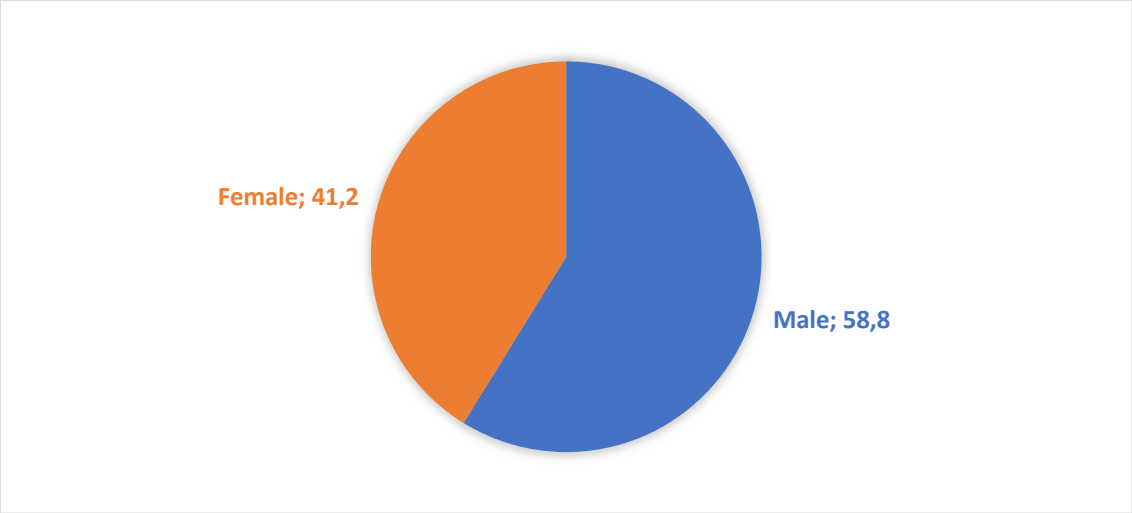

Figure 1. Gender Distribution of Respondents

Figure 1 illustrates the gender distribution of 371 respondents in the respondent pool from Kabul University. It revealed that most of the respondents were male students, who represented 218 respondents (58.8%), in contrast to 153 females, comprising 41.2% of the sample. Overall, this gender sample distribution indicates that male students were more involved in the study than females and reflects the overall enrollment patterns that are often seen across similar higher educational classroom settings in Afghanistan. However, since both male and female students were included in the sample, the findings provide checks in perspectives, informing a more reliable and representative analysis of cybersecurity awareness and practice through the lens of gender.

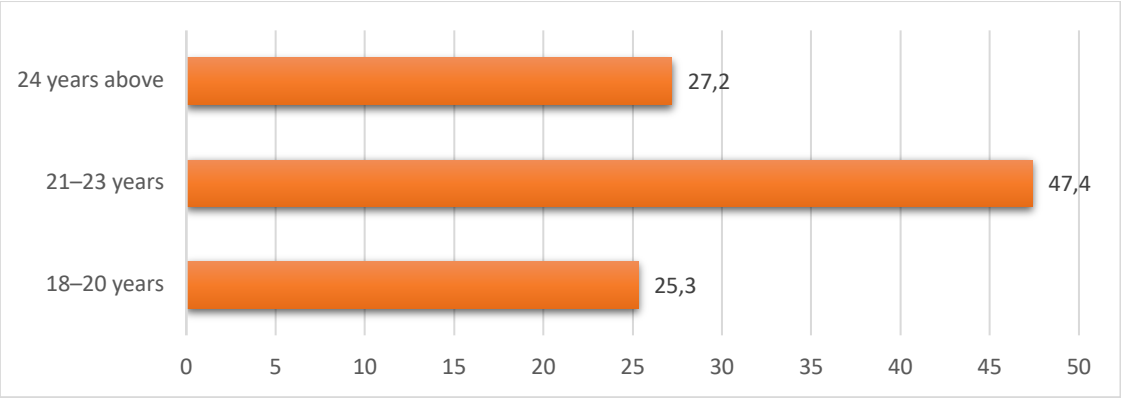

Figure 2. Age Distribution of Respondents

The age distribution of respondents in Figure 2 shows the largest group of participants was in the age range of 21–23 years (176 students, or 47.4%); a group which likely reflects the normal age of first-year undergraduate students at Kabul University. The second largest group of respondents was students aged 24 years and above (101 respondents, or 27.2%). This likely includes university students who may have entered university later than others, and/or took a break from their studies before starting university. There were also 94 respondents (25.3%) in the younger cohort of 18–20 years

of age. Overall, the distribution provided many case-historical variations in educational background, which are an asset to the study findings on cybersecurity awareness.

Table 1. Validity of the Cybersecurity Awareness Survey Instrument

Domain	Item No.	Factor Loading
Cybersecurity Knowledge	K1	0.78
	K2	0.81
	K3	0.75
	K4	0.80
Attitude toward Cybersecurity	A1	0.82
	A2	0.79
	A3	0.77
Secure Cyber Practices	P1	0.74
	P2	0.76
	P3	0.79

Researchers validated the survey instrument to measure students' cybersecurity knowledge, attitudes, and secure practices accurately. The validated instrument was reviewed for content validity by a panel of specialists in cyber-security and education, ensuring the items' relevance and clarity on a 5-point Likert scale. Validity was assessed by conducting exploratory factor analysis, with factor loadings from .74 to .82, which exceed the desired 0.50 threshold. The findings demonstrate that all items strongly represent their domains, confirming the reliability and interpretability of subsequent analyses. By including the validated instrument, the study is more rigorous and findings about the students' cybersecurity awareness and behavior are more credible.

Table 2. Reliability of Survey Instrument

Domain	Number of Items	Cronbach's Alpha
Cybersecurity Knowledge	4	0.83
Attitude toward Cybersecurity	3	0.81
Secure Cyber Practices	3	0.79
Overall Instrument	10	0.84

The reliability of the cybersecurity awareness survey instrument was evaluated using Cronbach's Alpha to examine the internal consistency across all domains. Differences in reliability were evident in the individual domain analyses, with the Cybersecurity Knowledge domain reaching an alpha of 0.83, Attitude toward Cybersecurity reaching 0.81, and Secure Cyber Practices reaching 0.79. The Cronbach's Alpha for the instrument as a whole was 0.84; all values exceed the commonly accepted threshold for reliability of 0.70, thereby indicating high internal consistency. Collectively, these results suggest the survey items are reliable and provide consistent measurement of intended

constructs that will support the credibility and dependability of the descriptive and inferential analyses of cybersecurity knowledge, attitudes, and practices of students.

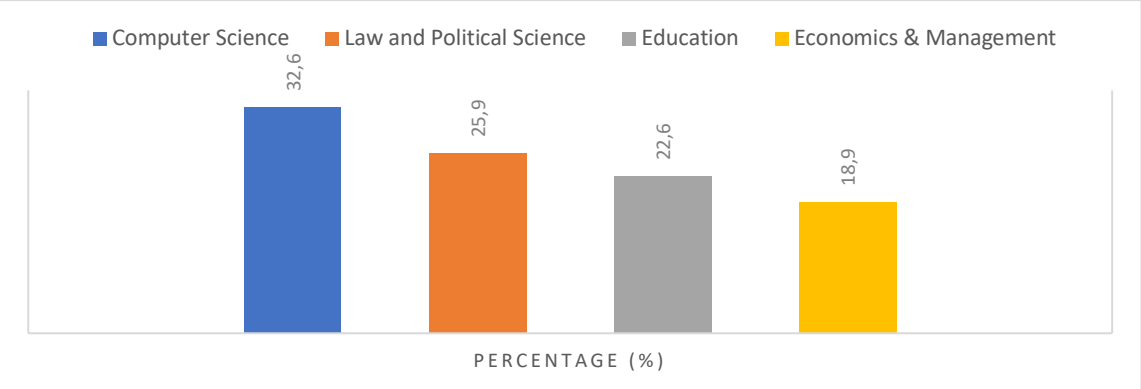

Figure 3. Faculty-wise Distribution of Respondents

The distribution of respondents by faculty is summarized in Figure 3, indicating the varied representation of students from Kabul University. The largest proportion of participants was from the Faculty of Computer Science, with 121 students (32.6%); this can be anticipated, as these students would have direct engagement with digital technologies, and thus would be the most familiar with issues related to cybersecurity. The Faculty of Law and Political Science represented 96 respondents (25.9%), a reflection of the increased focus in academia on matters of cyber law. The Faculty of Education represented 84 students (22.6%), indicating the role of future educators in promoting students' digital literacy and safe practices. Finally, 70 students (18.9%) came from the Faculty of Economics and Management, representing students who are more heavily reliant on digital tools to complete tasks based in finance and administration. This distribution was necessary to hear about cybersecurity awareness from several academic perspectives and to support the validity and generalizability of the study's findings.

Descriptive Analysis of Cybersecurity Awareness

Table 3. Descriptive Statistics of Cybersecurity Knowledge, Attitudes, and Practices

Variable	Mean	Std. Deviation	Min	Max
Cybersecurity Knowledge Score	3.74	0.82	1	5
Attitude toward Cybersecurity	3.91	0.71	2	5
Secure Cyber Practices Score	3.56	0.88	1	5

Table 3 displays the descriptive statistics of respondents' cybersecurity knowledge, attitudes, and practices. The mean score for cybersecurity knowledge was 3.74 (SD = 0.82) on a 5-point scale indicating a moderate level of knowledge regarding basic cybersecurity concepts. The attitude toward cybersecurity had the highest mean score at 3.91 (SD = 0.71), indicating that respondents generally have a good attitude and perception of the importance of cybersecurity in both educational and personal contexts. The secure cyber practices score was slightly lower at 3.56 (SD = 0.88), indicating respondents have some awareness of cybersecurity and value its importance,

but their secure practices do not align with their knowledge and attitude. There is an apparent gap between awareness and behavior, which is often a challenge in cybersecurity education. Overall, the findings show a need for targeted interventions to raise knowledge and encourage the implementation of secure digital practices.

Inferential Statistics

Table 4. Independent Samples t-test: Cybersecurity Awareness by Gender

Gender	Mean Score	Std. Dev.	t-value	p-value
Male	3.85	0.77	2.31	0.021*
Female	3.62	0.86		

*Significant at $p < 0.05$

The findings from an independent samples t-test measuring cybersecurity awareness between male and female students at Kabul University are reported in Table 4. Male students reported a higher mean score of 3.85 (SD = .77), compared to females' mean of 3.62 (SD = .86). The calculated t-value was 2.31 and a p-value of 0.021 indicates that the difference in mean scores is statistically significant at the 0.05 level. Therefore, these findings indicate that male students demonstrated significantly more cybersecurity awareness than female students. Such a distinction could reflect underlying differences in prior experience with digital technologies, academic preparation or engagement in computing- and computer programming-related activities. The findings noted above indicate there is a clear need for a gender-sensitive approach to awareness programs so that women students are equipped with appropriate training and support to enable their cybersecurity awareness and practice and thus diminish the gap in the cybersecurity awareness levels.

Table 5. One-Way ANOVA: Cybersecurity Awareness Across Faculties

Source	Sum of Squares	df	Mean Square	F-value	p-value
Between Groups	12.41	3	4.14	5.72	0.001**
Within Groups	265.82	367	0.72		
Total	278.23	370			

Post-hoc analysis: Students in Computer Science reported significantly higher awareness than those in Education and Economics.

Table 5 displays the one-way ANOVA analysis examining the differences in cybersecurity awareness across the faculties at Kabul University. The results are statistically significant with faculty showing a significant difference in levels of awareness, as the between-groups sum of squares was 12.41, the mean square was 4.14, the F-value was 5.72, and the p-value was 0.001, indicating significance at the $p<0.01$. The sum of squares and mean square of 265.82 and 0.72 were reported within groups for a total sum of squares of 278.23. The Tukey post hoc comparisons provided the information that students in the Faculty of Computer Science had significantly greater awareness related to cybersecurity than their peers in the Faculty of Education and the Faculty of Economics

& Management. The current results support the assumption that awareness and knowledge may be increased simply by exposure to specific disciplines and/or curricula related to cybersecurity. Therefore, awareness programs should be tailored to meet the needs of students, particularly those who have experienced lower levels of exposure to courses related to technology and systems.

Table 6. Chi-Square Test: Recognition of Phishing Emails by Gender

Gender	Recognized (%)	Not Recognized (%)	χ^2-value	p-value
Male	65.1	34.9	6.43	0.011*
Female	50.3	49.7		

*Significant at $p < 0.05$

Table 6 summarizes the Chi-square results concerning recognized phishing emails by Kabul University students by sex. As shown in Table 9, 65.1% of male students recognized phishing emails compared to only 50.3% for female students, while 34.9% of males did not detect phishing attempts compared to 49.7% for female students. The χ^2-value was 6.43, with a p-value of 0.011. This indicates a statistically significant relationship between gender and phishing email recognition at the 0.05 alpha level. It appears that male students are more proficient than female students in recognizing phishing emails. The gender observations provide an opportunity to focus on targeted interventions for enhanced cybersecurity awareness in which female students can be helped to improve phishing detection skills to be safer online and reduce vulnerabilities to cyber incidents.

Table 7. Regression Analysis: Predictors of Secure Cybersecurity Behavior

Predictor Variable	β Coefficient	Std. Error	t-value	p-value
Cybersecurity Knowledge	0.41	0.08	5.13	0.000**
Attitude toward Cybersecurity	0.29	0.07	4.14	0.000**
Awareness of Cyber Law	0.25	0.09	2.77	0.006*
Gender (Male=1, Female=0)	0.12	0.06	1.96	0.051

Model Summary: $R^2 = 0.42$, Adjusted $R^2 = 0.40$, $F(4,366) = 27.45$, $p < 0.001$

Table 7 presents the results of a multiple regression analysis that examined predictors of secure cybersecurity behavior in first-year students at Kabul University. The independent variables applied in the model included cybersecurity knowledge, attitude towards cybersecurity, cyber law awareness, and gender. The model was significant, $F(4,366) = 27.45$, $p < 0.001$, with an R^2 of 0.42 and an adjusted R^2 of 0.40, which indicates that approximately 40% of the variance in secure cybersecurity behavior is predicted by these predictors.

At an individual level, cybersecurity awareness was the greatest predictor ($\beta = 0.41$, $t = 5.13$, $p < 0.001$), suggesting that the greater the awareness of students regarding cybersecurity aspects, the greater the tendencies for them to engage in safe behavior.

Similarly, attitude towards cybersecurity also predicted safe behavior positively (β = 0.29, t = 4.14, p < 0.001), marking the boundary of how students view and follow practicing safe cyber habits. Cyber law awareness was also a significant predictor (β = 0.25, t = 2.77, p = 0.006), indicating that awareness of legal frameworks improves good behavior in the virtual platform. Gender made a marginal contribution (β = 0.12, t = 1.96, p = 0.051), suggesting male students are slightly more likely to have better cybersecurity behaviors than female students, although this effect wasn't statistically significant. These findings support the inclusion of knowledge enhancement, attitude acquisition, and cyber law know-how within education interventions to promote safe digital conduct among university students.

3.1. Discussion

The present study aimed to assess cybersecurity awareness, attitudes, and practices among first-year students in Kabul University and how specifically gender, faculty, and cyber law awareness influenced them. The demographic results reported a higher percentage of male students (58.8%) compared to female students (41.2%), consistent with Afghan higher education enrollment (Al-Janabi & Al-Shourbaji, 2016). Age distribution indicated a majority of the participants to be in the age group of 21–23 years, typical of the general undergraduate population, while faculty-wise distribution indicated the largest presence to be from Computer Science, nicely representing the highest exposure to technology among the study population (Cheng & Wang, 2022).

Descriptive analysis indicated that students possessed moderately high cybersecurity knowledge (M = 3.74, SD = 0.82) and positive attitudes towards cybersecurity (M = 3.91, SD = 0.71), but true secure practices were slightly lower (M = 3.56, SD = 0.88). This is also in line with existing research emphasizing awareness doesn't always translate to secure use of the internet (Ahmad et al., 2021; Al-Fatlawi, 2024). Students demonstrated a realization of key concepts such as phishing, social engineering, and good password needs but the application in practice is still inconsistent, mirroring the need for behavior reinforcement by training programs (Armas & Taherdoost, 2025).

Inferential statistics revealed significant gender variations, as men scored higher on awareness and phishing identification. This finding is also in line with earlier studies by Chang and Coppel (2020) and Oroni et al. (2025), which found that male students in developing countries show greater digital exposure and technological self-efficacy and therefore increased cybersecurity awareness. ANOVAs run likewise indicated Computer Science students to be far more aware than Economics and Education department students, validating the position of contact within field in determining cybersecurity skill (Kumar et al., 2024; Filipenko et al., 2025).

Regression analysis also confirmed cybersecurity knowledge, positive attitude, and cyber-law awareness as predictors of secure behavior. This corroborates earlier evidence indicating that legal framework awareness improves online-responsible conduct (Marune & Hartanto, 2021; Alwan, 2019). The gender variable had a marginal effect, whereby males have higher secure practices but the difference is less evident once knowledge and attitude are controlled for. These observations highlight the importance of comprehensive interventions that combine technical education, law

education, and attitude formation to establish sustainable cybersecurity habits among learners (Shillair et al., 2022; Sandi & van den Berg, 2025).

4. Conclusion

The investigation The study investigated first-year students' awareness, attitude, and behavior in relation to cybersecurity at Kabul University, specifically examining gender, faculty, and experience with cyber law. The findings indicated that students had moderate to high levels of knowledge of cybersecurity, as well as positive attitudes about safe behavior online. However, there was a considerable gap between what students indicated they knew and their actual behaviors online reflective of safe behavior, suggesting potential for more practice-based approaches to education. Male students and those in Faculty of Computer Science exhibited significantly higher knowledge than female students and students enrolled in non-technical faculties.

A notable outcome of the regression analysis was the finding that knowledge of cyber law was a significant predictor of secure cybersecurity behavior; this was important since it shows that cyber law is not on the periphery of digital behavior, but at its core. Legal knowledge provides students with an understanding of the potential outcomes of their actions in the digital space (data misuse, invasion of privacy, involvement in cybercrime), and to access knowledge of their rights and protections in the digital space.

There are distinct gaps in learning and teaching, and there is a pressing need for higher education institutions to teach cyber law/training as part of their cybersecurity curriculum. This activity should include a syllabus that included, but was not limited to, national and international data protection laws, cybercrime laws, and institutional policies concerning digital ethics, and digital accountability. Training in cyber law should be incorporated into the faculty of education's general education program and sequence and prioritized across a variety of learning scenarios (i.e., case studies, simulations, and inter-faculty, learning across all faculties while continuing to explore faculties beyond the disciplines of computer science or law). Gender-sensitive measures need to be prioritized to ensure that women students have access to legal and digital safety training comparable to their male peers.

In addition to curriculum reform, universities should develop institutional policies that mandate ongoing legal awareness training, particularly during student orientation programs and digital literacy workshops. Embedding cyber law into institutional policy frameworks ensures that cybersecurity is approached holistically—combining technical skills, behavioral insights, and legal understanding.

Ultimately, the findings highlight that effective cybersecurity education must go beyond teaching secure practices—it must build a culture of legal awareness and accountability. By institutionalizing cyber law as a foundational component of cybersecurity education, higher education can produce digitally literate graduates who are not only technically capable but also legally informed, ethically responsible, and better prepared to navigate the complex digital environments of the modern world.

Recommendations and Implications

From the findings of this research, it can be suggested that more work ought to be done in developing the cybersecurity culture around students at Kabul University. Cybersecurity education should be a part of all the faculties that have modules on phishing, social engineering, hacking, and cyber law, especially both theoretical content and practical work. Additionally, special focus should be given to female students and students from non-computing programs, such as Education and Economics, to mitigate the gender and faculty level awareness gaps observed. Awareness drives and education campaigns should promote positive cyber safety attitudes that will enhance the transformation of knowledge into safe web actions. There is also a need to increase awareness of cyber law, as knowledge of laws can promote responsible behavior and discourage risky internet behavior that can negatively affect individuals and society. It is also important to put theory into practice in relation to phishing detection training, one's own device security, password generation, and other safe habits. It is suggested that university administrations create institution-wide policies to support the culture of digital citizenship, which includes reporting recommendations for cyber incidents and providing opportunities for students to practice safe online behaviors.

The conclusions from this study have implications of the same magnitude. Scholarship-wise, the research highlights that knowledge alone is not sufficient without attitude development and practical skills, emphasizing the importance of holistic cybersecurity education. From a policy perspective, this research provides a basis for developing targeted policies which can be employed by universities with respect to the differences in faculty and gender and awareness and practice. Behaviorally, more awareness of the legal landscape and structured educational programs can positively influence the online interactions of students, reducing vulnerability to cyber-attacks and providing a safer online environment. Finally, the research creates opportunity for longitudinal studies and comparative studies of other university programs to compare how educational materials work as interventions and how the cybersecurity culture develops. Future research should explore longitudinal impacts of cybersecurity education, cross-university comparisons, technology-based interventions, and gender-specific awareness strategies.

References

Ahmad, N., Laplante, P. A., DeFranco, J. F., & Kassab, M. (2021). A cybersecurity educated community. IEEE Transactions on Emerging Topics in Computing, 10(3), 1456-1463. https://doi.org/10.1109/TETC.2021.3093444

Al-Fatlawi, H. H. M. (2024). Awareness of cyber security aspects in distance education. Journal of Pedagogical Sociology and Psychology, 6(1), 77-88. https://doi.org/10.33902/jpsp.202424403

Ali, G., Samuel, A., Mijwil, M. M., Al-Mahzoum, K., Sallam, M., Salau, A. O., ... & Melekoglu, E. (2025). Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey. Mesopotamian Journal of Computer Science, 2025, 115-158. https://doi.org/10.58496/MJCSC/2025/008

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. Journal of Information & Knowledge Management, 15(01), 1650007. https://doi.org/10.1142/S0219649216500076

Alwan, H. B. (2019). National cyber governance awareness policy and framework. International Journal of Legal Information, 47(2), 70-89. https://doi.org/10.1017/jli.2019.22

Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. Information, 16(5), 336. https://doi.org/10.3390/info16050336

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. Computers & Security, 97, 101959. https://doi.org/10.1016/j.cose.2020.101959

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192

Filipenko, N., Lukashevych, S., Andrieieva, O., Palkova, K., Rakstiņš, V., Juļa, L. (2025). Information Security Policy in Higher Education Institutions. In: Lytvynov, O., Pavlikov, V., Krytskyi, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2024. ICTM 2024. Lecture Notes in Networks and Systems, vol 1474. Springer, Cham. https://doi.org/10.1007/978-3-031-94852-7_11

Furnell, S. M., & Vasileiou, I. (2022). A holistic view of cyber security education requirements. In M. Khosrow-Pour (Eds.), Research anthology on advancements in cybersecurity education (pp. 289– 307). IGI Global. https://doi.org/10.4018/978-1-6684-3554-0.ch013

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417. https://doi.org/10.3390/info12100417

Kumar, A., Mishra, K., Mahto, R. K., & Mishra, B. K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. LatIA, 2, 94-94. https://doi.org/10.62486/latia202494

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. International Journal of Business, Economics, and Social Development, 2(4), 143-152. https://journal.rescollacomm.com/index.php/ijbesd/article/view/170

Oroni, C.Z., Xianping, F., Ndunguru, D.D. et al. Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. Educ Inf Technol 30, 14197–14236 (2025). https://doi.org/10.1007/s10639-025-13366-2

Pirinen, R., Rathod, P., Gugliandolo, E., Fleming, K., & Polemi, N. (2024, May). Towards the Harmonisation of Cybersecurity Education and Training in the European Union Through Innovation Projects. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-9). IEEE. https://doi.org/10.1109/EDUCON60312.2024.10578867

Sandi, S., & van den Berg, C. L. (2025). Cybersecurity mindset and upskilling: Resilience via lifelong learning and security education. South African Journal of Information Management, 27(1), 12. https://doi.org/10.4102/sajim.v27i1.2044

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., & Von Solms, B. (2023). Building cybersecurity capacity through education, awareness, and training. In Cybersecurity for decision makers (pp. 365-382). CRC Press. https://doi.org/10.1145/3344429.3372507

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. International Journal of STEM Education for Sustainability, 3(1), 47-67. https://www.journal.gmpionline.com/index.php/ijses/article/view/132