International Journal of Human and Society (IJHS)

E-ISSN: 2710-4966	P-ISSN: 2710-4958
Vol. 6. No. 01 (Jan-Mar) 2026	Page 375-398

https://doi.org/10.5281/zenodo.20256442

Cyber Hygiene Practices among University Students: A Comparative Study of Public and Private Institutions

Arsal Ajmal	BSCS, Air University Multan Campus, Islamabad arsal.ajmal621@gmail.com
Hanzala Bashir	BSCS, Air University Multan Campus, Islamabad hanzalabashir.71@gmail.com
Salman Khalid	BSCS, Air University Multan Campus, Islamabad salmankhalid2511@gmail.com
Khuzaim Adnan Qureshi	BSCS, Air University Multan Campus, Islamabad khuzaimadnana@gmail.com
Dr. Muhammad Arfan Lodhi **(Corresponding Author)**	Higher Education Department, Punjab Email: samaritan_as@hotmail.com

Abstract: *The academic experiences of university students in Pakistan are increasingly mediated by digital technologies, making cyber hygiene a critical component of safe and effective participation in higher education. Despite this shift, the cyber hygiene behaviors of students, particularly those studying in institutions located outside major metropolitan centers, remain insufficiently examined. This study investigates the cyber hygiene practices of undergraduate students enrolled in BSCS and IT programs across public and private universities in Multan. It aims to determine whether institutional type contributes to significant differences in cybersecurity related behaviors. An exploratory, quantitative research design was employed using a structured questionnaire consisting of 30 items measured on a five-point Likert scale. The instrument assessed six key dimensions of cyber hygiene, including password management, data protection awareness, safe browsing practices, software update behavior, privacy policy engagement, and participation in cybersecurity training. A total of 77 students participated in the study, with 45 respondents from public universities and 32 from private institutions. Data were analyzed using comparative statistical techniques to evaluate differences between the two groups. The findings reveal that cyber hygiene practices among students are moderately developed but exhibit notable inconsistencies across specific dimensions. Contrary to common assumptions, no statistically significant differences were observed between students from public and private universities across all six dimensions. Both groups demonstrated relatively weaker behaviors in areas such as regular password updating, reviewing privacy policies prior to application downloads, and engagement in institution-led cybersecurity training programs. These results suggest that institutional resources alone do not guarantee better cybersecurity practices among students. The findings contribute to the growing discourse on digital literacy and cybersecurity in developing academic environments and provide a foundation for future empirical and policy-oriented research.*

Keywords: Cyber hygiene; cybersecurity awareness; university students; password management; Protection Motivation Theory; digital security behavior; Pakistan

1. Introduction

Cybersecurity can no longer be considered something that only affects governmental institutions and large corporations. Students attending university often over unreliable connections face cybersecurity problems on a daily basis, including accessing cloud learning programs, submitting homework assignments via institutional platforms, communicating via various channels, and performing financial transactions using their smart phones. However, how effectively and safely they accomplish such tasks still lacks comprehensive studies, especially in developing nations where the spread of technology occurs faster than the introduction of cybersecurity education into the curriculum. This study seeks to investigate the practices of university students enrolled in both private and public institutions of Multan, Pakistan, in six categories of cyber hygiene behavior and see if institution type plays any role in their cyber hygiene practices.

1.1 Background of the study

In the process of digitizing education, there have been real pedagogical benefits as well as an increase in vulnerability areas. The learning management system, online tests, cloud collaboration applications, and digital submission systems are now defining elements in the lives of students from around the world. Information related to students' performance and even their personal information flows through networks of varying security strength, without knowledge on the part of many students. Cyber hygiene is the term used for the collection of behaviors that people regularly engage in to safeguard themselves from harm and protect their information and identities both online and offline. The similarity with personal health is intended, as washing one's hands on a daily basis is sufficient to prevent infections and illnesses without needing expert medical knowledge, while using complex passwords and backing up files are examples of activities that shield the average user from the most prevalent risks without requiring any special technical skills. The concern, which is reflected uniformly across all research studies, is that college students fail to cultivate such behaviors (Cain et al., 2018; Neigel et al., 2020). The cybersecurity context of Pakistan introduces country-specific factors to these issues. As per the report by Pakistan CERT, there was a significant increase in cyberattacks against academic networks from 2019 to 2022, whereby compromise, phishing attacks, and social engineering account were found to be the most prevalent threats in universities (Pakistan Computer Emergency Response Team, 2022). In his study, Shad (2019) noted that cyberbullying and account compromise were common among students in Pakistani universities, while institutions had been responding reactively and inconsistently to such issues. The directives from the Higher Education Commission on digital literacy have yet to result in any curricular requirement for institutions in this regard. There exist notable disparities in terms of IT infrastructure, personnel, and curricula in public and private universities of Pakistan, which may influence students differently in digital safety awareness.

1.2 Rational of the Study

One basic problem is yet to be solved in the research based upon cybersecurity education in Pakistani universities that majority of the students would attend a private university, which has better financial resources and IT infrastructure, lead to significantly improved security practices? All of the previous studies have focused on one university or type of cyber threats, providing insufficient information for decision-makers. Therefore, this study seeks to fill this void by comparing the students from public and private universities in Multan via a six-dimensional behavioral scale. Despite increased attention being paid to this topic at a global level, Pakistan-specific comparative research studies analyzing students' cyber security behaviors are relatively rare. Even where such studies exist, they tend to be limited in scope to measuring the prevalence of cyber bullying (Shad, 2019) or awareness of single threats instead of comprehensively measuring the complete behavioral range. While Fatima et

al. (2023) conducted an analysis of cyber security awareness among students studying in three universities in Islamabad; they did not use institutional type as their main point of comparison. There are no existing studies that used a validated multidimensional measure to analyze the cyber behaviors of public versus private university students in Multan, to the authors' knowledge.

1.3 Research Objectives

1. To evaluate and compare the levels of cyber hygiene behavior of undergraduate students enrolled in public as well as private universities in Multan, Pakistan.
2. To find out if there are any statistical significant differences in behavior on six aspects among public and private universities' students
3. To find out the worst aspect of cyber hygiene behavior among both categories of students in public and private sector universities

1.4 Research Questions

1. What is the average level of cyber hygiene practices observed among undergraduate students enrolled in both public and private universities in Multan?
2. Are there any significant differences in cyber hygiene practices of students in public and private universities, measured against six different criteria?
3. In which areas are cyber hygiene practice the poorest and what are the institutional differences in the observed trends?

1.5 Hypotheses

The affirmative and null hypotheses for the current study are given as under:

1. H1: There is a significant difference in the overall composite scores for cyber hygiene between the students of public and private universities in Multan, Pakistan.
2. Ho: There is no significant difference in the overall composite scores for cyber hygiene between the students of public and private universities in Multan, Pakistan.

2. Literature Review

2.1 Theoretical Framework

Three different theories provide the foundation for this research, each bringing an unique element of explanation as to why learners engage in or refrain from engaging in digital safety practices. The relationship between these theories is depicted in Figure 1 below.

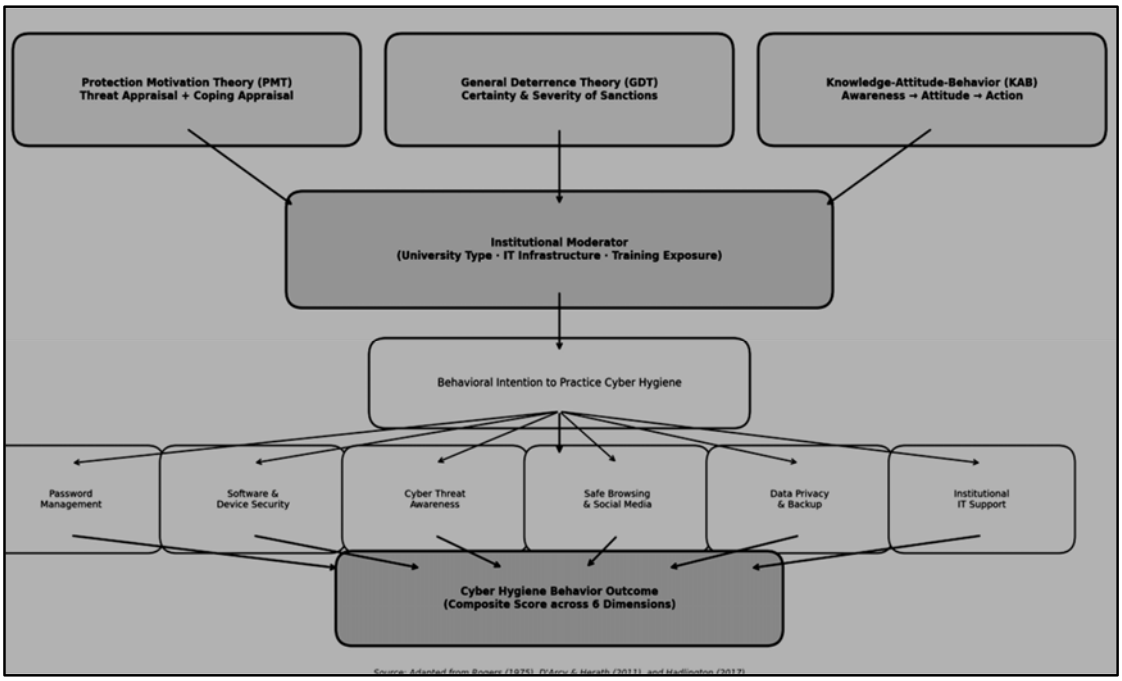

Figure 1. Concept Map 1: Integrated Theoretical Framework

The Protection Motivation Theory (PMT), formulated by Rogers (1975) and further refined by Maddux and Rogers (1983), defines protective behavior in terms of two cognitive appraisals acting in concert. The first one is threat appraisal, which refers to a personal perception of the seriousness and the likelihood of the threat. The other one is coping appraisal, meaning a personal judgment on whether the protection strategies are viable and adequate enough for mitigating the threat. If both assessments score sufficiently high, the probability of behavioral adaptation is increased dramatically. Applied to the case of cyber hygiene, the student perceiving the potential danger posed by phishing attempts and considering the process of carefully checking links realistic is much more likely to engage in such behavior. Numerous empirical investigations confirm the predictive power of PMT when it comes to cybersecurity behaviors (Boss et al., 2015; Tsai et al., 2016; Luse et al., 2013).

General Deterrence Theory (GDT) modified for cybersecurity context through D'Arcy and Herath (2011) suggests that deterrence depends on how likely individuals perceive a penalty will be for failing to abide by certain security standards. Within the scope of a university institution, the more students think that careless conduct in cyberspace will result in penalties, the greater the probability of taking protective measures. Moreover, it becomes evident that when policy statements are made on paper, without any implementation or communication, no deterrent effect can be achieved.

The KAB Model, which has been employed in the study of cybersecurity education by Hadlington (2017), constitutes the third level of explanation. According to the KAB theory, behavior change cannot be achieved simply through the acquisition of knowledge. First, knowledge needs to alter attitudes, and secondly, the newly created attitudes need to translate into action. It is possible for a student to know that password reuse is a bad practice without having developed an attitude that prompts them to adopt the opposite stance on it. It is the logical process behind why the same paradox has been repeatedly observed; that of the technically competent student continuing to exhibit risky behavior.

2.2 Empirical Studies

Overall, the body of research related to the cybersecurity behaviors of students does not

only state the fact that cybersecurity practices are not perfect. Rather, it shows that the knowledge-practice gap is an integral part of how cybersecurity education operates, regardless of the country's cultural context, type of institution involved, and the level of computer skills possessed by learners. The basis for this statement is presented in Cain et al. (2018), whose research of undergraduate students from five American colleges showed that those participants who could correctly recognize phishing in theoretical tasks were unable to use this knowledge in practical actions on the internet. This was especially obvious in terms of password management and multi-factor authentication, skills that require effort to implement but do not imply any conscious recognition of their importance. Neigel et al. (2020) expanded this notion further and added objective measurements of users' behavior alongside their self-reports, proving that college students usually have an inflated opinion of their personal cybersecurity. For survey-based papers such as the current one, the meaning of this statement is evident and straightforward: mean values from self-report measures can be considered optimistic, which implies even lower actual values. What is perhaps most interesting about the longitudinal studies by Barakovic and Husic (2022, 2023, 2024), performed on several Bosnian universities, is the level of rigor in their methodology for determining which interventions have been truly effective in modifying behavior. The authors' longitudinal approach revealed that any structured training in cybersecurity, even if only brief, yielded a substantial increase in behavior, compared to controls who were never trained. However, it is notable that annual awareness days which did not integrate into the curriculum failed to produce any effect on long-term modification. This conclusion leaves little doubt when it comes to policy implications. Torten et al. (2016) reached the same conclusion via a completely different path, demonstrating that behavior reverted almost immediately to baseline following one awareness session in Australia.

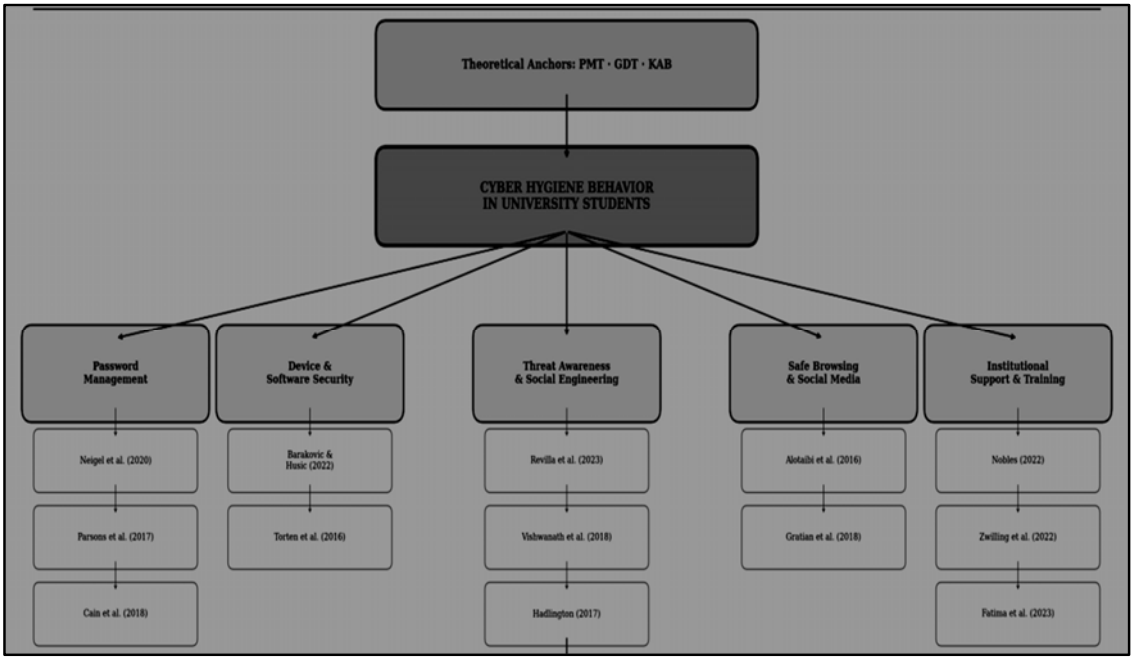

Figure 2. Concept Map 2: Literature Review Structure

The comparative institutional literature is just as enlightening. In South Africa, Chandarman and Van Niekerk (2017) observed slight differences in scores between private institution users and their peers, with the former doing slightly better on device protection and Internet security behavior, which was attributed to more training and better IT resources at those institutions. However, this advantage was small and not large as would be expected by the presence of more

resources. Academic field, according to Alotaibi et al. (2016), had a greater impact on behavior in Saudi universities than the type of university with STEM majors consistently outperforming their counterparts in social sciences in terms of security behavior. Parsons et al. (2017), while validating their questionnaire for Australia, similarly found little moderating influence of organization type in security behavior. Threat-specific research supports this argument from a different perspective. In a study conducted using a simulation to examine students' phishing susceptibility at Spanish universities, Revilla et al. (2023) found that cybersecurity education rather than computer literacy determined whether an individual would be able to avoid phishing attacks. Vishwanath et al. (2018) established that individuals who were used to checking their emails in a careless way were more susceptible to phishing because they paid less attention while reading than others. Therefore, despite spending more time using digital technologies, such people are not better equipped to protect themselves from cyberattacks. According to Hadlington (2017), this should be seen as a human factor issue because lapses in security are caused by cognitive inattention and impulsivity rather than ignorance.

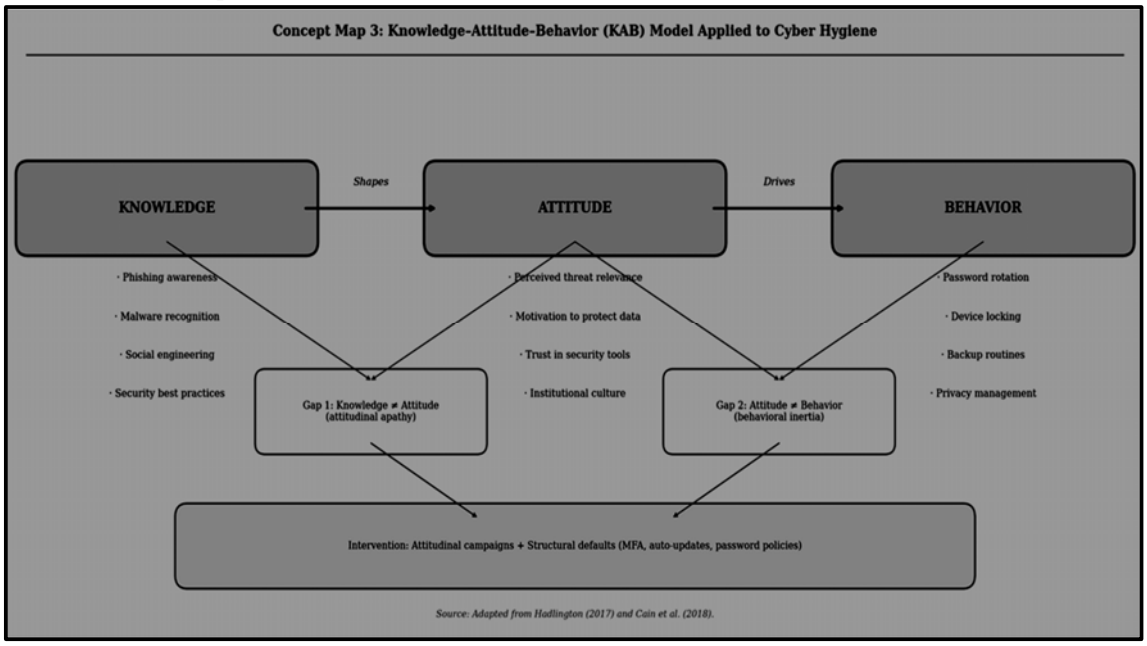

Figure 3. Concept Map 3: KAB Model Applied to Cyber Hygiene

Pakistani and regional findings provide the specific grounding for these arguments in light of the current study. For example, according to Fatima et al. (2023), although the awareness regarding cybersecurity among the students from Islamabad University was average, their behavior and organizational support of IT was found to be poor. Similarly, Shad (2019) noted that the response of educational institutions had been reactive as opposed to preventive regarding the problem of account compromise and cyberbullying. This has set a precedent that is confirmed by the current study through data presented in section G. According to Zwilling et al. (2022), final year students of computer science from Eastern Europe showed no advantage over first-year students.

This is perhaps the most pointed finding in the entire literature: technical curriculum, without explicit behavior-targeted instruction, does not produce behavioral improvement even in students who have spent years studying computing. Gratian et al. (2018) add a dispositional dimension, showing that conscientiousness rather than technical knowledge was the strongest personality predictor of secure behavior, suggesting that effective training programs must account for individual differences rather than treating all students as uniform recipients of information. At

the policy scale, Nobles' (2022) systematic review across fifteen countries confirms that curriculum-embedded, assessed cybersecurity modules were the single most consistently effective intervention, dwarfing the impact of standalone workshops or orientation sessions. And this is perhaps one of the most direct insights to emerge from the entire body of research: the mere inclusion of technical education within a curriculum without deliberate behaviorally-oriented training fails to engender any change in behavior, even among students who have been exposed to computing for several years. As further proof of this, Gratian et al. (2018) offer a dispositional element by demonstrating that conscientiousness—not technical competence—was the most important predictor of security practices among personalities. Policy-wise, a systematic review carried out by Nobles (2022) in 15 different countries found that assessed cybersecurity education integrated into curricula emerged as the most consistently effective intervention by far.

2.3 Conceptual Framework

The independent variable in this research is the institution type, defined as the membership of universities to either public or private institutions. The main dependent variable in this analysis is cyber hygiene behavior, which is defined as an aggregate score generated from 30 Likert scale questions distributed among six dimensions of cyber hygiene behavior: password hygiene, software/device security, awareness of cyber threats, online and social networking behavior, data privacy/backup, and utilization of institutional IT services. The university type serves as the moderating variable, whose theory suggests that its impact will be exerted on individuals' behavior indirectly by means of training, infrastructure, and policies. The pathway from individual awareness to behavior has been designed using the KAB model, motivational factors have been captured by PMT, and institutional repercussions are included in GDT.

3. Methodology

3.1 Research Design

Quantitative-descriptive research methodology is used for this paper. Quantitative cross-sectional surveys facilitate data gathering among different subjects simultaneously, providing a basis for statistical analysis without the need for longitudinal studies. This approach describes behavior patterns at a certain point in time and determines whether there are any significant differences among them according to sectors of institutions.

3.2 Population and Sampling

In this study, the targeted population includes undergraduate students studying BSCS and other IT courses in universities situated in Multan, Pakistan. The selection of this city is purposeful since it is an intermediate city having relatively developed academic technological facilities which can be considered to be a very large class of Pakistani universities that generally remain out of the research focus on the major cities like Islamabad, Lahore, and Karachi. The recruitment process used stratified random sampling in order to have equal representation from both institutional categories. Prior to the collection of data, a power analysis was conducted which revealed that the minimum sample size required for an independent-samples t-test was 64 participants ($d = 0.5$, $\alpha = 0.05$, power = 0.80). A total of 77 participants were recruited, 45 (58.4%) from public universities and 32 (41.6%) from private universities.

3.3 Instrumentation

The main instrument used in collecting data was a 34-questionnaire consisting of several sections. Section A contained four questions in terms of demographics. Sections B to G contained five questions each, covering all six dimensions discussed in the theoretical framework of cyber hygiene behavior. All behavioral and attitudinal questions were measured using a Likert scale of one to five, where one is ‘strongly disagree’ while five is ‘strongly agree’. This study’s questionnaire instrument was based on that by Parsons et al. (2017) and Barakovic& Husic (2023).

3.4 Validity and Reliability

Content validity was established through peer review by two instructors who are experts in cybersecurity teaching and survey methods. Each question was checked for comprehension, relevancy, and construct consistency; three questions were modified based on their advice. Face validity was tested using cognitive interviews with five BSCS students. A trial test with twenty students yielded a Cronbach's Alpha of 0.84, well above the cut-off point of 0.70. Full-scale testing yielded a Cronbach's Alpha of 0.899 for all thirty behavior questions.

3.5 Data Collection Procedure

The survey was conducted electronically using Google Forms for a period of three weeks in March 2026. Respondents were selected from official WhatsApp groups and portals associated with the selected universities. All potential respondents were provided an information sheet regarding the objective of the research and the voluntary participation of the respondent. The confidentiality and anonymity policy was discussed beforehand. Informed consent was sought from all respondents before including them. Ethical approval was taken from the department of Air University Multan Campus, and no financial benefits were involved.

3.6 Data Analysis Techniques

Statistical analyses were all performed on IBM SPSS Statistics 26. Mean, standard deviation, and frequencies (% distribution) were obtained for every individual item and every behavior dimension based on institution type. Independent-samples t-test was used to determine whether significant group differences existed, considering an alpha level of 0.05 to be statistically significant. Pearson correlation analysis was performed to test the relationship between selected awareness and behavior dimensions and the composite score. Cohen's d was estimated along with every t-test value to provide insights on the effect size of group differences in addition to statistical significance.

4. Results

4.1 Demographic Analysis

Table 1. Demographic Distribution of the Sample (N = 77)

Variable	Category	Frequency	Percentage
University Type	Public University	45	58.4%
	Private University	32	41.6%
Gender	Male	65	84.4%
	Female	12	15.6%
Age Group	18-20 years	18	23.4%
	21-23 years	32	41.6%
	24-26 years	21	27.3%
	27 years or above	6	7.8%
Department	Computer Science / IT	29	37.7%
	Business / Management	12	15.6%

	Engineering	11	14.3%
	Social Sciences / Arts	5	6.5%
	Other	20	26.0%
Total		77	100%

Note. Percentages are rounded to one decimal place.

Out of 77 participants, most (58.4%) belonged to government-run colleges. Moreover, the sample had a significantly higher proportion of male participants (84.4%). This distribution is quite common among computing program enrollments in Pakistanian universities, according to Fatima et al. (2023). Participants aged between 21 to 23 (41.6%) and 24 to 26 (27.3%) made up the majority of the sample, which can be considered normal for an undergraduate population. Out of all the participants, the biggest proportion came from Computer Science and IT (37.7%), although Business and Social Sciences were also represented.

4.2 Descriptive Statistics

Table 2. Section B — Password Management

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q5: Unique password per account	10.4	13.0	24.7	28.6	23.4	3.42 (1.27)	3.33	3.53
Q6: Complex password composition	3.9	9.1	14.3	35.1	37.7	3.94 (1.12)	3.93	3.94
Q7: Regular password rotation	13.0	31.2	18.2	20.8	16.9	2.97 (1.32)	2.80	3.22
Q8: Use of password manager	5.2	14.3	26.0	29.9	24.7	3.55 (1.16)	3.33	3.84
Q9: Avoid sharing passwords	9.1	14.3	13.0	22.1	41.6	3.73 (1.37)	3.96	3.41
Section B Composite						3.52	3.47	3.59

Note. SD = Strongly Disagree; D = Disagree; N = Neutral; A = Agree; SA = Strongly Agree; M = Mean. Q7 registered the lowest mean in the entire questionnaire.

Complexity of the password (Question #6, Mean = 3.94) is the highest-scoring item in Section B, with 72.8% of participants responding positively. The most poorly performing item across the whole survey was routine password changes (Question #7, Mean = 2.97). It is the

only item that scored below the neutral mean score of 3.0. Just 37.7% of participants said they changed their passwords frequently enough, but 44.2% of participants disagreed. The use of password managers (Question #8, Mean = 3.55) demonstrated significant differences among the groups, with private college students scoring 0.51 points higher than public college students (Mean = 3.84 vs. 3.33).

Table 3. Section C — Software Updates and Device Security

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q10: OS updated to latest version	3.9	11.7	18.2	32.5	33.8	3.81 (1.15)	3.82	3.78
Q11: Regular app/software updates	5.2	5.2	16.9	41.6	31.2	3.88 (1.08)	3.80	4.00
Q12: Antivirus/anti-malware use	9.1	15.6	27.3	27.3	20.8	3.35 (1.23)	3.22	3.53
Q13: Device locking when unused	1.3	7.8	18.2	33.8	39.0	4.01 (1.01)	4.02	4.00
Q14: Avoid unlicensed software	3.9	19.5	27.3	26.0	23.4	3.45 (1.16)	3.40	3.53
Section C Composite						3.70	3.65	3.77

Note. Q13 (device locking, M = 4.01) was the highest-scoring item in the entire questionnaire, consistent with its reinforcement by smartphone default settings.

Device Locking (Q13, M = 4.01) ranks highest in both Section C and the complete questionnaire, with 72.8% either agreeing or strongly agreeing. It is safe to assume that the findings have very little to do with the individual's conscious effort in making decisions regarding cybersecurity measures but rather, that it is simply the smartphone's default screen lock behavior. The weakest measure in this section would be the use of an antivirus program (Q12, M = 3.35), since only 48.1% agree.

Table 4. Section D — Cyber Threat Awareness: Frequency Distribution and Mean Scores (N = 77)

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q15: Recognize phishing/suspicious links	2.6	11.7	19.5	49.4	16.9	3.66 (0.98)	3.73	3.56
Q16: Aware of ransomware/malware	5.2	15.6	19.5	40.3	19.5	3.53 (1.13)	3.47	3.62
Q17: Know social	1.3	13.0	41.6	27.3	16.9	3.45 (0.97)	3.40	3.53

engineering attacks								
Q18: Report suspicious cyber activity	3.9	27.3	19.5	31.2	18.2	3.32 (1.17)	3.22	3.47
Q19: Stay informed on cybersecurity news	3.9	16.9	27.3	29.9	22.1	3.49 (1.13)	3.36	3.69
Section D Composite						3.49	3.44	3.57

Note. Q17 produced the highest neutral response rate in the entire questionnaire (41.6%) suggesting social engineering remains a less familiar concept than discrete threats such as phishing or ransomware.

Item Q15 on phishing recognition (M = 3.66) emerges as the highest rated item in section D, receiving agreement or strong agreement from 66.3% of respondents, possibly due to media reports about phishing being a well-known issue. The item with the highest concern level is incident reporting (Q18, M = 3.32), with 31.2% of participants disagreeing with the idea of reporting suspicious behavior. This finding validates GDT's claim that lack of an enforcement mechanism would result in non-compliance to institutional security protocols. Social engineering (Q17) elicited the largest number of neutral answers out of all items in the questionnaire (41.6%), indicating that even though phishing is well-known, its more general concept as social engineering is not understood by many students.

Table 5. Section E — Safe Browsing and Social Media Behavior

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q20: Avoid unknown links/pop-up ads	6.5	3.9	20.8	29.9	39.0	3.91 (1.16)	4.07	3.69
Q21: Use HTTPS for personal information	3.9	7.8	19.5	42.9	26.0	3.79 (1.04)	3.62	4.03
Q22: Careful about social media	2.6	7.8	15.6	40.3	33.8	3.95 (1.02)	3.91	4.00
Q23: Review social media privacy settings	1.3	18.2	20.8	29.9	29.9	3.69 (1.13)	3.58	3.84
Q24: Avoid public Wi-Fi for sensitive use	10.4	24.7	22.1	24.7	18.2	3.16 (1.28)	3.00	3.38
Section E Composite						3.70	3.64	3.79

Note. Q24 produced the most concerning distribution in this section, with 35.1% disagreeing with avoiding public Wi-Fi for sensitive transactions.

For Section E, it is important to note that it carries both the second highest composite mean score (equal to that of Section C at 3.70) as well as one of the most concerning findings in this survey. Among all items in this section, the avoidance of public Wi-Fi for carrying out

sensitive transactions (Q24, M = 3.16) comes as the lowest, with 35.1% of the participants either disagreeing or strongly disagreeing with this statement. Considering the fact that public Wi-Fi is available extensively throughout Pakistan in different academic institutions and public locations, this poses a behavioral risk indeed.

Table 6. Section F — Data Privacy and Backup Practices

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q25: Regular data backups	6.5	14.3	29.9	33.8	15.6	3.38 (1.11)	3.42	3.31
Q26: Read privacy policies before install	7.8	29.9	24.7	23.4	14.3	3.06 (1.20)	3.00	3.16
Q27: Limit app permissions	2.6	7.8	26.0	41.6	22.1	3.73 (0.98)	3.80	3.62
Q28: Delete unused apps/accounts	2.6	13.0	19.5	45.5	19.5	3.66 (1.02)	3.69	3.62
Q29: Mindful of data shared online	3.9	7.8	19.5	44.2	24.7	3.78 (1.03)	3.78	3.78
Section F Composite						3.52	3.54	3.50

Note. Q26 (privacy policy reading, M = 3.06) was the second-lowest scoring item in the entire instrument, with 37.7% disagreeing.

Read privacy policy (Q26, M = 3.06) is a second-weakest element on this list, with 37.7% of respondents actually agreeing. This is an example of a behavior that requires conscious decision and an effort made by the individual before they can take any action, precisely what the KAB theory says people will avoid when there is no attitudinal commitment to it. Backup data regularly (Q25, M = 3.38) is a third-weakest item. The last point worth noting is that, unlike in any other section, public university students performed slightly better than private university students in Section F.

Table 7. Section G — Institutional IT Support

Item	SD% (1)	D% (2)	N% (3)	A% (4)	SA% (5)	Overall M (SD)	Public M	Private M
Q30: University provides cybersecurity training	15.6	23.4	23.4	26.0	11.7	2.95 (1.27)	3.00	2.88
Q31: IT dept helps with cyber threats	13.0	19.5	27.3	26.0	14.3	3.09 (1.25)	2.98	3.25
Q32: University has clear tech-use policies	13.0	15.6	29.9	24.7	16.9	3.17 (1.26)	3.29	3.00
Q33: University prepares students for	16.9	13.0	27.3	28.6	14.3	3.10 (1.29)	3.20	2.97

online safety								
Q34: Willing to attend cybersecurity workshops	6.5	11.7	14.3	36.4	31.2	3.74 (1.21)	3.78	3.69
Section G Composite						3.21	3.25	3.16

Note. Q30 is the only item in the entire questionnaire to fall below the neutral midpoint (M = 2.95). The contrast with Q34 (student willingness to attend workshops, M = 3.74) reveals an implementation gap:

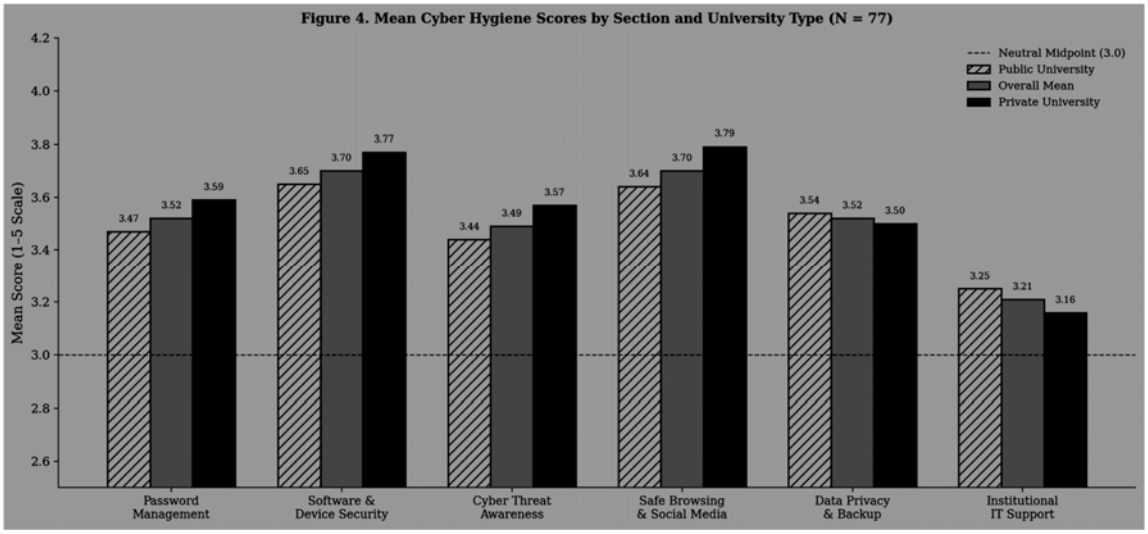

Figure 4. Mean Cyber Hygiene Scores by Section and University Type (N = 77)

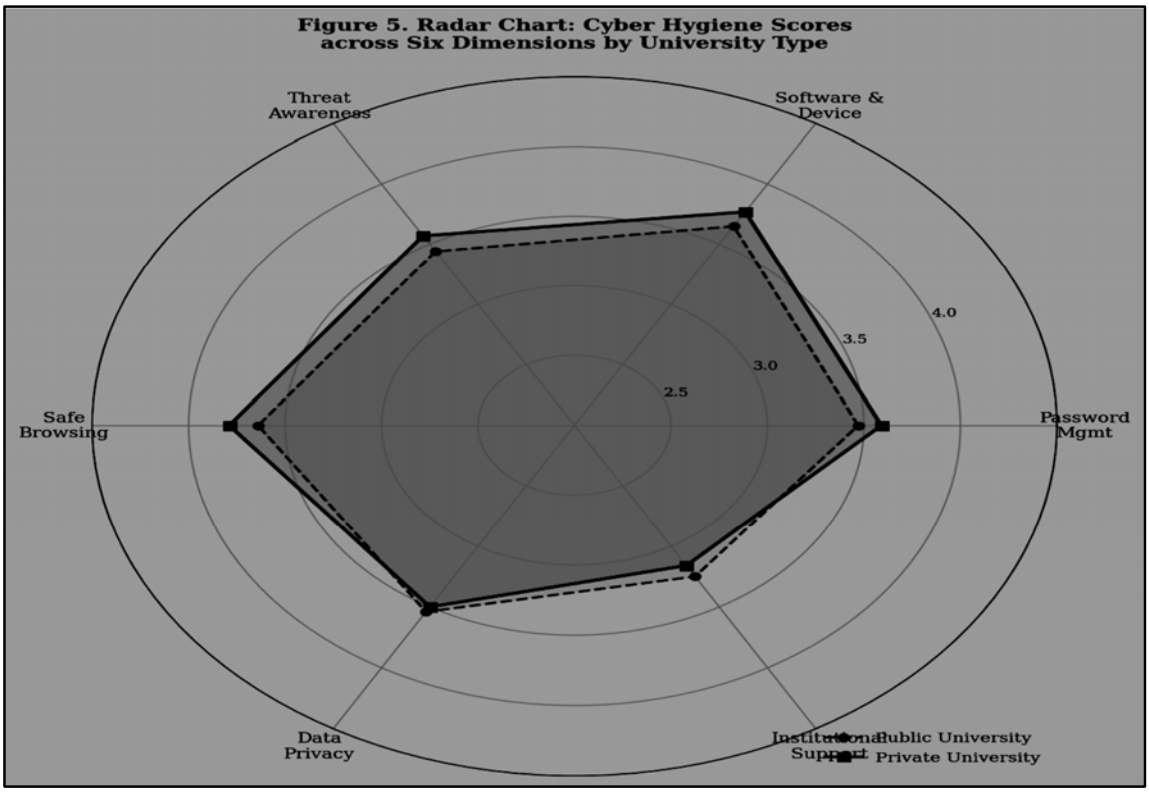

Figure 5. Radar Chart: Comparative Cyber Hygiene Profiles across Six Dimensions

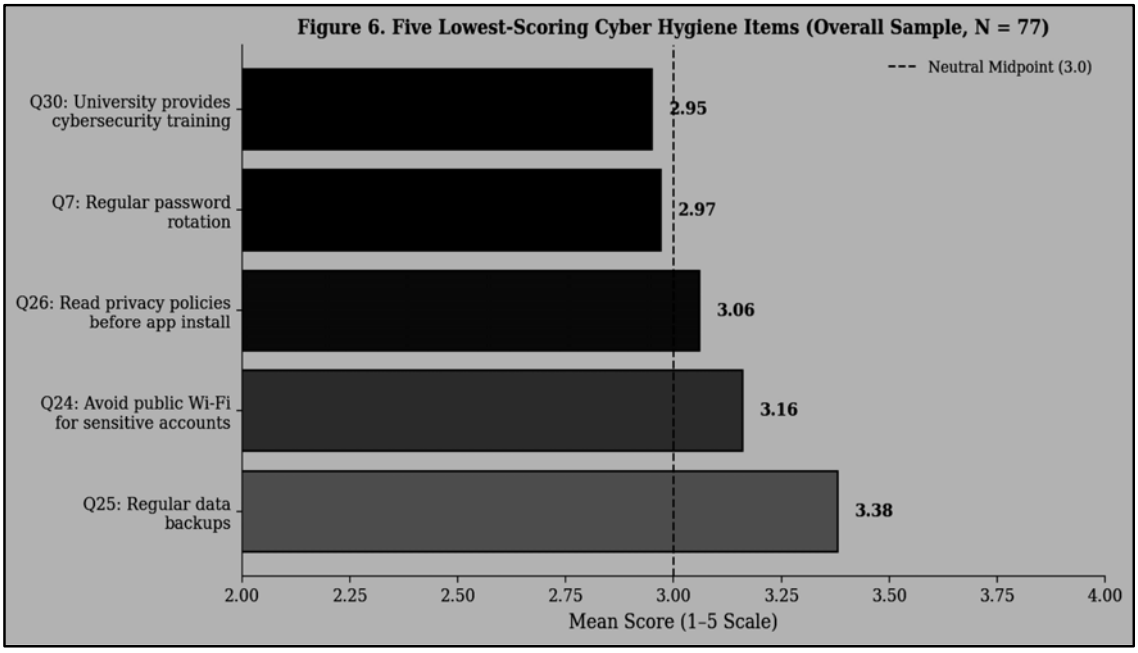

Figure 6. Five Lowest-Scoring Cyber Hygiene Items across the Full Sample (N = 77)

The last section, Section G, was the least scoring on average in this study (M=3.21) and arguably, it is the most significant in terms of analysis because of its implications for policy formation. Training for cybersecurity (Questionnaire Item 30, M=2.95) is the single question in this study that scored below the neutral level on both public and private students equally (both scored 3.00). As much as 39.0% of the students disagreed or strongly disagreed with the notion that the university provided training to increase cybersecurity awareness among students. Contrast this with Questionnaire Item 34 where 67.6% of students agreed or strongly agreed to be engaged in training if offered (M=3.74).

4.3 Inferential Statistics

Table 8. Independent-Samples t-Test Results by Section and University Type (N = 77)

Section	Overall M	Public M	Private M	t	df	p	Cohen's d
B: Password Management	3.52	3.47	3.59	-0.72	69.0	.474	0.10
C: Software & Device Security	3.70	3.65	3.77	-0.67	61.8	.503	0.11
D: Cyber Threat Awareness	3.49	3.44	3.57	-0.80	65.5	.427	0.13
E: Safe Browsing &Social Media	3.70	3.64	3.79	-0.87	72.9	.386	0.12
F: Data Privacy & Backup	3.52	3.54	3.50	0.24	56.3	.808	0.04
G: Institutional IT Support	3.21	3.25	3.16	0.40	51.9	.693	0.07

Overall Composite	3.53	3.50	3.56	-0.47	58.9	.642	0.07

Note. All p-values are two-tailed. No comparison reached significance at $p < .05$. Cronbach's Alpha = .899 ($k = 30$, $N = 77$). Cohen's $d < .20$ across all comparisons indicates negligible effect sizes. t-statistics computed using Welch's correction for unequal variances.

Table 9. Pearson Correlations: Selected Items vs. Overall Composite Score (N = 77)

Variable Pair	Pearson r	Interpretation
Ransomware/Malware Awareness (Q16) vs. Composite	0.712	Strong positive
Stay Informed on Cybersecurity (Q19) vs. Composite	0.575	Moderate positive
Device Locking Habit (Q13) vs. Composite	0.549	Moderate positive
Phishing Recognition (Q15) vs. Composite	0.547	Moderate positive
University Training Provision (Q30) vs. Composite	0.522	Moderate positive
Social Engineering Knowledge (Q17) vs. Composite	0.431	Moderate positive

Note. All correlations are significant at $p < .001$ (two-tailed). Composite = mean of all 30 behavioral items.

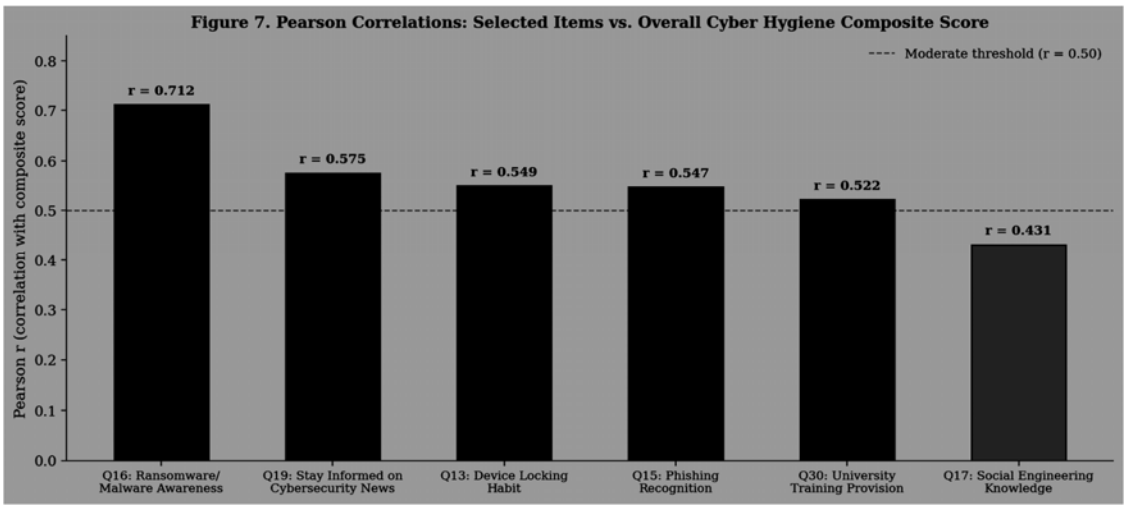

Figure 7. Pearson Correlations: Selected Items vs. Overall Cyber Hygiene Composite Score

As shown in Table 8, results from independent samples t-test analysis conducted for all six sections as well as for overall composite did not yield any statistically significant difference between public universities' students versus private universities' students. The overall composite mean scores for public university respondents and private university respondents were 3.50 and 3.56 respectively, representing a difference of 0.06 and negligible effect size ($t = -0.47$, $df = 58.9$, $p = .642$, Cohen's $d = 0.07$). H1 is rejected; null hypothesis H0 is accepted. The variable which is most strongly correlated to the overall behavioral composite score is "general cyber threat awareness" (Q16, $r = 0.712$).

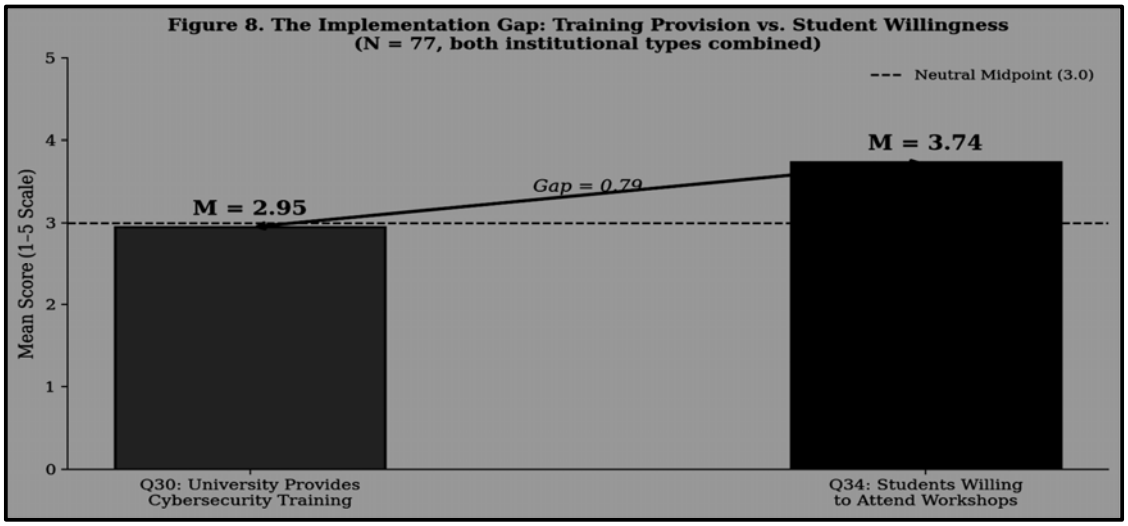

Figure 8. The Implementation Gap: Institutional Training Provision vs. Student Willingness to Participate

5. Discussion

The results reveal a more nuanced reality about the cybersecurity consciousness of Pakistani students than what a rosy or grim interpretation would imply. All of them scored above the neutral point in five out of six categories, suggesting a fairly favorable attitude towards secure online practices. They are certainly not a bunch of individuals who lack knowledge regarding cybersecurity. Expected effects due to differences in institution type were not observed. For all six behavioral dimensions as well as for the composite average, both groups exhibited no significant difference. There is no statistically significant difference between the means of the composite average by 0.06, which bears neither statistical nor practical significance using any standard measurement of effect size. It is consistent with the findings of Chandarman and Van Niekerk (2017) from their study conducted in South Africa and the results obtained by Parsons et al. (2017) from their study involving different organizations in Australia; institutional affiliation does not play a significant role in determining the behavior of the respondents. Institutional factors like resources, better IT units, updated technology, or specialized teaching staff do not necessarily lead to better safety behavior on part of the students. Predictors in this case behave individually. The best predictor for the overall composite is cyber threat awareness (r = 0.712), an aspect that depends on the PMT threat appraisal process.

The actual weakness demonstrated in both cases has just as much value as the lack of impact by institution-based policies. Password updates (M = 2.97) and review of the privacy policy (M = 3.06) were the least performed activities in terms of performance. Both involve self-regulation which takes effort without instant payoffs or cues from the environment. It is not about awareness – students recognize that both are necessary activities. The problem lies in a discrepancy between attitudes and actions, and awareness campaigns are not enough to bridge the gap. Default settings for automated password changes, mandatory two-step authentication for institutional sites, preconfigured backups minimize the individual's effort in the process while offering an external incentive which cannot be achieved through voluntary self-regulation alone. This is proven by Barakovic and Husic (2023) and Torten et al. (2016). Behavioral regression occurs after any awareness-only campaigns; defaults make it stick.

The analysis in section G provides the most straightforward policy recommendation based on the findings. The only survey question with an average score lower than the midpoint neutral value was that related to institutional provision of training programs (Q30), which scored equally for both public and private university participants (3.00 compared to 2.88). This

finding is of analytical significance because it demonstrates that the problem of lack of training opportunities in cybersecurity is not specific to any particular category of universities and cannot be solved through the reassignment of funds within these institutions. Rather, this is a general issue affecting higher education institutions in Pakistan, which is further proven by the difference between the scores in question Q30 and those in the question regarding the willingness to attend such training sessions (Q34, M = 3.74). According to Nobles (2022), the most effective measure of increasing cybersecurity among students is the introduction of relevant courses.

The difference between habit-driven actions and deliberate actions, which is evident from the item-level data, requires further consideration in itself. Device Locking (Q13, M=4.01) and being careful about one's personal information when using social media (Q22, M=3.95) are two high-scoring actions that are part of people's day-to-day interactions with digital devices and are reinforced by the default settings on these devices. On the other hand, password change, privacy policy review, reporting incidents, and data backup are four low-scoring actions that entail making deliberate and periodic choices, but are not environmentally reinforced.

6. Implications

6.1 Practical Implications

Institutions in both public and private sectors must incorporate cybersecurity literacy modules that are mandatory and graded for BSCS and IT degrees. These modules should include topics such as password safety practices, recognition of phishing scams, safe internet browsing, hazards of using public Wi-Fi, backing up data, and application permission control. IT departments within institutions must simultaneously implement structural defaults like multi-factor authentication in academic platforms, automatic password reset, screen lock enforcement, and device updates. Collaboration with Pakistan CERT must be made formal to offer phishing simulation drills and threat intelligence briefings.

6.2 Theoretical Implications

Null result on the institutional type indicates empirical evidence in support of the KAB model's key thesis that behavior modification necessitates an attitude change rather than only resource availability. The strong positive relationship between threat awareness and total composite score (r = 0.712) affirms PMT's mechanism of threat appraisal as a reliable predictor of behavior in the university setting in Pakistan. Symmetrical shortage of institutional support in both sectors indicates that GDT's hypothesis holds true in predicting the loss of deterrence where no enforcement is perceived to exist.

6.3 Policy Implications

The Higher Education Commission needs to establish national minimum standards for cybersecurity education for all undergraduate computing courses with behavioral assessment outcomes being part of accreditation requirements as opposed to relying on voluntary compliance. These standards need to include specific contact hours, assessment methods, and behavioral performance criteria as opposed to mere awareness. The research literature is consistent in indicating that curriculum integrated approaches to education have a sustained impact on behavior while separate workshops fail (Nobles, 2022; Torten et al., 2016).

7. Limitations

There are various limitations involved in the interpretation of these results. The foremost of these concerns the fact that these findings have been based entirely upon self-reported behavioral measures, which are subject to bias due to social desirability effects. According to Neigel et al. (2020), it was found empirically that students tend to overreport the level of security practices followed by them as compared to objective behavioral audits; therefore, the reality may actually be less than what is depicted through these average scores. It restricts the scope to other cities within Pakistan, or even outside of it, especially the countryside regions. The skew towards male students, which accounted for 84.4%, may imply different behaviors by male and female students, which

may have been undetected in this research. The use of a cross-sectional research design limits us from observing how behavior changes over time with increasing knowledge and changing policies.

8. Conclusion

The present research study assessed the cyber hygiene practices of 77 students of BSCS and IT degree programs from both private and government universities situated in the city of Multan in Pakistan, using a reliable 30-item scale measuring password hygiene, software and device security, awareness of cybersecurity threats, secure browsing, data protection, and university-based IT assistance. These results support an understanding of partial cyber hygiene behavior adoption where students demonstrate positive orientation towards being safe on the internet, but fail to adopt behavior involving active and periodic effort. The null hypothesis was not upheld in the study. Students from public and private universities could not be differentiated in all six behaviors and the total behavior score. The private university students scored slightly higher in most of the sections, although the gap between the scores could not be considered statistically or practically significant. The private universities' resource edge did not give them an advantage in behavioral security. The most readily actionable aspect from this study would be the symmetric deficiency in training identified in Section G, whereby both sectors had an equally poor showing as against the midpoint value on the scale in terms of training in cyber security, and both sectors showed an equally keen interest in attending training seminars in the event of their availability. The difference in the willingness of the students to attend training seminars and the unwillingness of the institutions to conduct such seminars is easily reconcilable, and does not simply involve adjustments in policy, but a paradigm shift in the approach to cyber security within Pakistan’s higher education sector.

9. Recommendations

Longitudinal studies that track the same group of people through multiple academic years will show how cyber hygiene behaviors develop and if certain interventions lead to lasting behavior change, which can be studied neither by longitudinal nor by cross-sectional survey studies. Experimentation designs where one group is subjected to cyber hygiene training modules and another group to regular training will give us the causation that correlation data may offer. Research conducted across the country in different areas, including Lahore, Karachi, Islamabad, and rural universities, would allow for national comparisons. Research involving students from other disciplines, such as the humanities, social sciences, and professional courses, will provide an overview of behavior in the wider student population. In addition to survey tools, objective behavioral measures, phishing test susceptibility tests, device audit logging, or web browser activity could minimize the self-report biases. High and low scoring participants should be interviewed to understand underlying causes.

10. References

Alotaibi, F., Roussinov, D., Lotfi, A., Stewart, W., Creighton, J., & Alzahrani, A. (2016). Cybersecurity behaviors among university students in Saudi Arabia. In Proceedings of the Science and Information Conference (SAI). IEEE.

Barakovic, S., & Husic, J. B. (2022). Survey on cyber hygiene among university students. In Proceedings of the 30th Telecommunications Forum (TELFOR). IEEE. https://doi.org/10.1109/TELFOR56187.2022.9983688

Barakovic, S., & Husic, J. B. (2023). Longitudinal assessment of cybersecurity behavior change after awareness training among university students. Journal of Information Security and Applications, 74, 103447. https://doi.org/10.1016/j.jisa.2023.103447

Barakovic, S., & Husic, J. B. (2024). Determinants of cyber hygiene compliance in higher education: A three-year panel study. Computers & Security, 138, 103657.

https://doi.org/10.1016/j.cose.2024.103657

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and coping appraisals for security adoption. MIS Quarterly, 39(4), 837-864. https://doi.org/10.25300/MISQ/2015/39.4.5

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication, 20, 133-155. https://doi.org/10.23962/10539/23572

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658. https://doi.org/10.1057/ejis.2011.23

Fatima, R., Ali, S., & Nawaz, M. (2023). Cybersecurity awareness among university students in Pakistan: Behavioral gaps and institutional responses. Pakistan Journal of Information Technology, 22(1), 45-62.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Enck, W. (2018). Correlating human traits and cyber security behavior intentions. Computers & Security, 73, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Higher Education Commission of Pakistan. (2021). National Curriculum Revision Committee guidelines for cybersecurity literacy integration. HEC Publications.

Luse, A., Mennecke, B., & Triplett, J. (2013). Determining the changing nature of phishing attacks through an analysis of recent phishing attacks. Issues in Informing Science and Information Technology, 10, 305-317.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. Computers & Security, 92, 101731. https://doi.org/10.1016/j.cose.2020.101731

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA Journal of Business and Public Administration, 13(1), 49-72. https://doi.org/10.2478/hjbpa-2022-0003

Pakistan Computer Emergency Response Team. (2022). Annual cybersecurity threat report 2021-2022. CERT-PK.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The influence of organizational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making, 11(1), 67-80. https://doi.org/10.1177/1555343416652025

Revilla, M., Zavala, J., & Lozano, C. (2023). Phishing vulnerability and prior cybersecurity training among university students: A simulated phishing experiment. Computers in Human Behavior, 140, 107577. https://doi.org/10.1016/j.chb.2022.107577

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Shad, I. A. (2019). Cyberbullying among university students in Pakistan: Prevalence, patterns, and institutional responses. Pakistan Journal of Criminology, 11(2), 56-72.

Torten, R., Reaiche, C., & Boyle, S. (2016). The impact of security awareness training: A systematic literature review. Computers & Security, 56, 157-169. https://doi.org/10.1016/j.cose.2015.09.002

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security, 59, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146-1166. https://doi.org/10.1177/0093650215627483

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97. https://doi.org/10.1080/08874417.2019.1680959

Appendix

Survey Form

Topic: Comparative Study of Cyber Hygiene Practices among Public and Private University Students

Respected Participant,

We are BSCS students at Air University Multan Campus, conducting a research study on cyber hygiene practices. All information collected will be kept strictly confidential and used solely for academic research purposes. No personal identification will be disclosed. Participation is completely voluntary and you may withdraw at any time without penalty.

Instructions: Please read each statement carefully and tick the option that best represents your practice or opinion. There are no right or wrong answers. Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

SECTION A: DEMOGRAPHIC INFORMATION

1. Gender: (1) Male (2) Female (3) Prefer not to say

2. Age: (1) 18-20 years (2) 21-23 years (3) 24-26 years (4) 27 years or above

3. University Type: (1) Public University (2) Private University

4. Program: (1) Computer Science/IT (2) Engineering (3) Business/Management (4) Social Sciences/Arts (5) Other: _____

SECTION B: PASSWORD MANAGEMENT PRACTICES

Statement	1	2	3	4	5
5. I use a unique password for each of my online accounts.	□	□	□	□	□
6. My passwords contain a mix of letters, numbers, and special characters.	□	□	□	□	□
7. I change my passwords regularly (at least every 3-6 months).	□	□	□	□	□
8. I use a password manager to store and manage my passwords securely.	□	□	□	□	□
9. I avoid sharing my passwords with friends or classmates.	□	□	□	□	□

SECTION C: SOFTWARE UPDATES & DEVICE SECURITY

Statement	1	2	3	4	5
10. I keep my operating system updated to the latest version.	□	□	□	□	□
11. I regularly update the apps and software installed on my devices.	□	□	□	□	□
12. I use antivirus or anti-malware software on my devices.	□	□	□	□	□
13. I lock my devices (phone/laptop) when not in use.	□	□	□	□	□
14. I avoid using unlicensed or pirated software on my devices.	□	□	□	□	□

SECTION D: AWARENESS OF CYBER THREATS

Statement	1	2	3	4	5
15. I can recognize a phishing email or suspicious link.	□	□	□	□	□
16. I am aware of common cyber threats such as ransomware and malware.	□	□	□	□	□
17. I know what social engineering attacks are and how to avoid them.	□	□	□	□	□
18. I report suspicious cyber activity to relevant authorities or IT staff.	□	□	□	□	□
19. I stay informed about the latest cybersecurity news and trends.	□	□	□	□	□

SECTION E: SAFE BROWSING & SOCIAL MEDIA BEHAVIOR

Statement	1	2	3	4	5
20. I avoid clicking on unknown links or pop-up advertisements.	□	□	□	□	□
21. I only use secure (HTTPS) websites when entering personal information.	□	□	□	□	□
22. I am careful about what personal information I share on social media.	□	□	□	□	□
23. I review the privacy settings of my social media accounts regularly.	□	□	□	□	□
24. I avoid using public Wi-Fi for accessing sensitive accounts (e.g., banking).	□	□	□	□	□

SECTION F: DATA PRIVACY & BACKUP PRACTICES

Statement	1	2	3	4	5
25. I regularly back up my important files and data.	□	□	□	□	□
26. I read privacy policies before installing new apps or signing up for services.	□	□	□	□	□
27. I limit the permissions I grant to mobile apps (e.g., location, contacts).	□	□	□	□	□
28. I delete apps and accounts I no longer use to reduce data exposure.	□	□	□	□	□
29. I am mindful of the data I share when using online platforms or services.	□	□	□	□	□

SECTION G: INSTITUTIONAL SUPPORT & CYBER HYGIENE TRAINING

Statement	1	2	3	4	5
30. My university provides cybersecurity awareness	□	□	□	□	□

training or workshops.					
31. The IT department at my university helps students with cyber threats.	□	□	□	□	□
32. My university has clear policies regarding the use of technology on campus.	□	□	□	□	□
33. I feel that my university adequately prepares students for online safety.	□	□	□	□	□
34. I would participate in cyber hygiene workshops if offered by my university.	□	□	□	□	□

Thank you for your kind participation.