Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 2, May 2026, pp. 619~630
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i2.pp619-630

Assessing cybersecurity awareness and security practices among university students in Jordan

Khader Musbah Ismail Titi
Department of Cybersecurity, College of Science and Information Technology, Irbid National University, Irbid, Jordan

Article Info

Article history:

Received Feb 3, 2025
Revised Mar 9, 2026
Accepted May 1, 2026

Keywords:

Behavioral in cybersecurity
Cybersecurity awareness
Cybersecurity best practices
Proper security tools usage
Security practices assessment

ABSTRACT

This paper sets out to evaluate the degree to which Jordanian university students genuinely comprehend and apply cybersecurity principles in their everyday digital lives. The rationale for undertaking this investigation is compelling: as cyber threats continue to intensify and diversify, remarkably little granular evidence exists to identify which sub-populations within the Jordanian student body are most vulnerable due to knowledge gaps. A structured survey reaching 150 students recruited from a range of academic departments served as the empirical foundation, with all quantitative analyses conducted using SPSS and MS-Excel. The analysis examined three demographic dimensions: gender, academic discipline, and geographic origin (urban versus rural). Students enrolled in computing and information technology programmes consistently demonstrated superior preparedness relative to their peers, and urban-based students exhibited more robust awareness profiles than those from rural areas. Building on these findings, the paper makes a case for systematic awareness programmes and for embedding cybersecurity content into curricula across all disciplines rather than restricting it to technical fields.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Khader Musbah Ismail Titi
Department of Cybersecurity, College of Science and Information Technology, Irbid National University
Irbid, Jordan
Email: k.titi@inu.edu.jo

1. INTRODUCTION

The rapid proliferation of digital technologies across all aspects of daily life — from mobile devices and cloud-based platforms to institutional portals and social media networks — has fundamentally transformed how university students engage with information and communication systems. This pervasive connectivity brings substantial academic and social benefits, yet it simultaneously exposes students to a growing and increasingly sophisticated threat environment. Cybersecurity, once a concern confined to IT specialists and network engineers, has evolved into a fundamental form of personal literacy required by anyone operating in the connected world [1]. At a technical level, the discipline encompasses the full spectrum of hardware, software, and procedural safeguards deployed to protect systems and networks against unauthorised access, disruption, and data loss. When any of these protections are deficient or absent, adversaries — opportunistic, criminal, or state-sponsored — are quick to exploit the resulting vulnerabilities. Malware campaigns, phishing schemes, and ransomware incidents have all escalated in complexity and volume in recent years, inflicting tangible harm on individuals and organisations across all sectors [2].

Protecting the technological infrastructure underpinning contemporary life — encompassing software stacks, hardware platforms, and the communication networks that support daily digital activity — demands sustained, coordinated effort. Perimeter defences, identity and access management, and continuous

behavioural monitoring of network traffic are widely recognised as indispensable elements of any credible security strategy [3]. Yet technical hardening of infrastructure alone cannot address the most persistent and consistently exploited vulnerability in organisational security: human behaviour. A substantial body of research confirms that actions such as clicking on malicious links, reusing passwords across accounts, and ignoring software update notifications collectively account for a disproportionate share of successful attacks. University students, given the intensity and diversity of their digital engagement, represent a particularly important population in this context. One might expect this technology-immersed cohort to be relatively well-prepared against cyber threats; the available evidence, however, presents a more nuanced picture, with security awareness found to vary significantly depending on a student's academic background and whether security education has been formally embedded in their degree programme [4]. There is broad consensus in the literature that cultivating this awareness prior to students entering the workforce is both achievable and essential [5].

The present paper reports the findings of an empirical investigation designed to address this challenge in a specific and relatively underexplored national context — Jordan. Drawing on student participants across multiple universities, the study sought to quantify cybersecurity awareness levels and to examine how three demographic variables — gender, academic major, and geographic background — shape those levels. The practical motivation is straightforward: when awareness profiles are found to vary in predictable ways across demographic subgroups, that knowledge equips universities to design targeted, cost-effective interventions that can meaningfully improve security behaviour throughout the student population [6].

At the outset of the study, three research questions were defined to give the inquiry a specific and tractable orientation:

a) Q1. How comprehensively do university students in Jordan understand information security concepts and translate that understanding into practice?
b) Q2. Does a student's gender, field of study, or place of residence have a measurable bearing on how well they understand and apply information security in Jordan?
c) Q3. In what ways do students at Jordanian universities value information security, and what obstacles prevent them from consistently practising it in their everyday digital routines?

Five sections organise the paper's content. Section 2 surveys the relevant literature on cybersecurity awareness, with particular attention to educational and regional contexts. Section 3 details the data collection and analytical procedures. Section 4 presents and interprets the empirical findings. Section 5 draws the paper to a close through a synthesis of the key conclusions, an honest appraisal of the study's limitations, and directions for future inquiry. Together, these sections are designed to equip Jordanian higher education institutions with a clearer and more actionable understanding of student cybersecurity awareness.

Despite the growing reliance of university students on digital technologies, limited empirical research has examined cybersecurity awareness and daily security practices among students in Jordanian universities. Understanding these behaviours is essential for designing effective, context-sensitive cybersecurity education programmes. Therefore, this study aims to assess cybersecurity awareness, password practices, phishing recognition, and device security behaviours among university students in Jordan, with the goal of informing targeted institutional interventions.

2. RELATED WORKS

Cybersecurity awareness has developed into a well-established research area since its emergence in the academic mainstream, with the accumulated literature now spanning diverse populations, industries, and geographic contexts. Several distinct research threads within this body of work are particularly pertinent to the questions addressed in the current study, and examining them provides a clearer sense of what the field has established and where meaningful gaps persist. One technically focused strand of the literature has engaged with the challenge of measuring situational awareness — the ability to perceive, interpret, and act on security-relevant events in real time. Al-Mohannadi *et al*. [7] offered an early and rigorous contribution in this area, constructing and validating a measurement instrument for cyber situational awareness among professional log analysts and establishing that such awareness was amenable to reliable quantification in operational environments. D'Amico *et al.* [8] examined the same theme from the vantage point of network security analysts, proposing a decision-support framework that integrated threat assessments, vulnerability indicators, and network stability metrics into a unified operational picture — on the premise that analysts working with such a framework would be better equipped to make sound, timely decisions.

Education-oriented research has applied comparably careful empirical methods to student populations. Al-Janabi and Al-Shourbaji [9] surveyed undergraduates, academic staff, and researchers at Middle Eastern institutions and produced findings that were at once sobering and practically informative:

participants demonstrated limited familiarity with basic information security principles and routinely conducted digital activities without apparent awareness of the associated risks. The conclusion that structured, institutionally coordinated training programmes were urgently needed resonated across subsequent contributions from other regions: Kritzinger and von Solms [10], Kumar *et al.* [11], and Alotaibi *et al.* [12] all documented comparable awareness deficits among university-level students and advanced targeted educational remedies. Workplace-focused research has consistently identified human behaviour as the vulnerability most readily exploited in organisational security chains. Alshaikh *et al.* [13] addressed this problem by designing the analyze-predict-aware-test (APAT) framework, which applied algebraic predictive modelling to anticipate employee-level vulnerabilities and inform proactive countermeasures. Alzahrani *et al.* [14] and Titi [15] applied similarly rigorous analytical approaches to the challenge of reducing security and privacy risks arising from employee errors in large-scale data environments. The recurring message across this strand of the literature is that effective awareness programmes must be sustained over time, contextually grounded in the learner's work environment, and reinforced by genuine organisational commitment.

Research originating within the Arab world has generated findings of direct relevance to the present study. Alotaibi *et al.* [16] surveyed internet users in Saudi Arabia and identified a pattern that has since appeared repeatedly across the region: strong general IT literacy coexisting with weak specific knowledge of threats and protective countermeasures. Aloul *et al.* [17] observed a similar tension in the UAE context and argued for targeted security education addressing both student and professional audiences, with particular attention to phishing awareness, wireless network security, and RFID-related risks. Quader and Janeja [18] significantly expanded the comparative scope with a multi-country study covering Palestine, Slovenia, Poland, and Turkey, reaching the conclusion that cultural and educational context exerts a shaping influence on cybersecurity behaviour that standardised, context-agnostic awareness campaigns are poorly suited to accommodate.

At a more theoretical level, Taherdoost [19] and Alazab and Broadhurst [20] addressed the methodological challenge of operationalising awareness as a quantifiable and cross-group comparable variable, proposing dynamic, capability-oriented models that introduced greater conceptual coherence into an otherwise fragmented literature. Contributions from Bangladesh by Islam *et al.* [21], Rahman *et al.* [22], and Hossain *et al.* [23], drawing on both online and offline survey methodologies, underscored the fact that inadequate public cybersecurity awareness is a challenge that extends far beyond higher education institutions and demands responses that integrate educational efforts with targeted policy measures. Surveying the breadth of this literature, the observation shared by Taherdoost [19] and von Solms and Van Niekerk [24] — that cybersecurity awareness will continue to demand sustained research attention in the years ahead, particularly in regions navigating accelerated digital transformation — offers a fitting frame for the Jordanian investigation that follows. While previous studies have focused primarily on general cybersecurity awareness, fewer have examined the relationship between demographic factors such as gender, academic discipline, and geographic origin and practical day-to-day security behaviours. Although several studies have investigated cybersecurity awareness among students in various national contexts, limited research has specifically focused on Jordanian university students and their real-world security practices across multiple behavioural dimensions, including password management, phishing recognition, and device protection. This study addresses that gap directly.

3. RESEARCH METHOD

Obtaining a trustworthy assessment of cybersecurity awareness — one that distinguishes between what student's report knowing and what they demonstrably do — demanded a research design capable of capturing both the declarative and behavioural dimensions of the construct. The methodological foundation of the investigation was descriptive and quantitative in character. The descriptive dimension enabled a detailed characterisation of the current state of cybersecurity awareness and practice among the sampled students, capturing the distribution of knowledge levels, the prevalence of specific security behaviours, and the variation in awareness profiles across demographic subgroups. The quantitative strand provided the statistical breadth necessary to detect patterns across a heterogeneous sample and to draw meaningful comparisons between student groups. Faculty perspectives in cybersecurity-adjacent departments were also incorporated through informal consultations, providing an external reference point against which self-reported student responses could be evaluated. Survey instruments were distributed across multiple Jordanian universities, with deliberate effort made to ensure disciplinary breadth in the resulting sample. The study engaged a total of 150 student participants; although this sample size is modest, it is considered sufficient for an exploratory awareness study of this nature and provides indicative insights into cybersecurity knowledge and practices among Jordanian university students. The questionnaire was distributed electronically using Google Forms, supplemented by WhatsApp-based course groups to extend reach across diverse academic

disciplines. The survey consisted of 24 items combining multiple-choice questions and four-point Likert-scale items, covering both cognitive awareness and reported security behaviours. The questionnaire was designed to capture responses from two key student groups: final-year students approaching graduation, whose cumulative academic experience positioned them well to reflect critically on the adequacy of their security preparation; and students across a range of disciplines, enabling comparison of security awareness between technical and non-technical fields. A total of 150 student participants were recruited from a range of academic departments, serving as the empirical foundation, with all quantitative analyses conducted using SPSS and MS-Excel.

3.1. Research design

The methodological foundation of the investigation was descriptive and quantitative in character. The descriptive dimension enabled a detailed characterisation of students' conceptual security knowledge, their capacity to recognise vulnerabilities, and their self-reported security practices. The quantitative dimension supplied the statistical apparatus required to assess the consistency of observed patterns and to compare outcomes across demographic subgroups with analytical rigour. The survey instrument was constructed to probe not only declarative knowledge but also behavioural orientations — specifically, whether students translated stated security convictions into actual protective conduct — as well as self-reported responses to concrete, real-world security scenarios. Operationally, the study was executed in five sequential steps: selecting participants from diverse disciplines, institutions, and backgrounds; administering the survey to this group; analysing responses to construct individual and group awareness profiles; guaranteeing all participants' voluntary participation and full anonymity; and designing the questionnaire to be completable within a 10 to 15 minute window.

3.2. Data sources

Primary data were collected through a structured student questionnaire distributed across multiple Jordanian universities. The questionnaire served a dual purpose — capturing students' conceptual understanding of cybersecurity principles and documenting their self-reported security behaviours in daily digital activities. The core dataset encompasses students drawn from multiple Jordanian universities and a cross-section of academic disciplines. Secondary material drawn from peer-reviewed journals, conference proceedings, academic texts, and established cybersecurity reports complemented the primary data, providing the theoretical grounding and comparative reference points needed to situate the primary findings within the broader scholarly conversation. Integrating these two data streams yielded an analysis that is simultaneously empirically robust and conceptually well-connected to the existing literature.

3.3. Questionnaire analysis

The primary data collection instrument comprised a 24-item questionnaire whose items were distributed across two thematic sections, each targeting a distinct dimension of cybersecurity awareness:

1. Knowledge, culture, and environmental awareness: Eleven closed-ended items probed students' conceptual understanding of core cybersecurity principles, their familiarity with threat categories, and the role their educational and social surroundings had played in shaping their awareness.
2. Behavioural dimension of awareness: Thirteen closed-ended items examined how students actually behave online — whether they use security tools consistently, how they respond when faced with potential threats, and whether their digital habits reflect their stated knowledge.

A four-point Likert format governed all responses: strongly disagree = 1, disagree = 2, agree = 3, strongly agree = 4. This format removed the escape route of a neutral midpoint, pushing respondents to take a position. The Likert responses were subsequently grouped into three interpretive categories (yes, no, and not sure) for simplified descriptive reporting in the results section. Completed responses were entered into SPSS version 20 for statistical processing, which enabled trend identification, subgroup comparison, and correlation analysis.

4. SURVEY RESULTS AND ANALYSIS

Data collection was conducted electronically, with Google Forms serving as the principal distribution platform owing to its accessibility and user-friendly interface. A supplementary distribution channel — course-linked WhatsApp groups operated by Irbid National University to facilitate student communication — extended the survey's reach and contributed to achieving disciplinary diversity within the final sample. Distribution arrangements were coordinated in advance with heads of department to ensure an orderly process that produced a sample authentically representative of multiple academic disciplines.

4.1. Quantitative and descriptive data analysis

Covering the full continuum from conceptual understanding to reported practice, the 24 survey items generated responses that were subsequently broken down by gender, place of origin, and field of study to permit meaningful comparisons between sub-groups. Table 1 that follows records how respondents were distributed across the three answer categories for each question:

Table 1. Distribution of respondent questions

Question	Yes (%)	No (%)	Not sure (%)
Do you have a working understanding of what "Information Security" means?	85%	10%	5%
Would you say that information security matters for keeping yourself safe on the internet?	90%	5%	5%
Have you installed protective software such as antivirus tools or a firewall on your devices?	70%	20%	10%
Do you keep up with developments and news related to cybersecurity risks?	60%	30%	10%
Do you actively take steps to safeguard your personal data online, such as updating your passwords?	75%	15%	10%
Are the passwords you create for your accounts difficult to predict or crack?	80%	10%	10%
Can you distinguish between computer viruses and other forms of malicious software?	65%	25%	10%
Do you consider public Wi-Fi networks to be safe to use?	55%	35%	10%
Are you familiar with the concept of two-step or two-factor verification (2FA)?	75%	15%	10%
Have you activated two-step verification on any of your online accounts?	60%	30%	10%
Do you apply the security guidance and advice issued by your online service providers?	70%	20%	10%
Do you keep your applications and operating system updated on a regular basis?	85%	10%	5%
Are you worried about the possibility of someone stealing your online identity?	80%	15%	5%
Do you create a unique password for each separate online account you hold?	65%	30%	5%
Is security software installed and active on your smartphone or tablet?	90%	5%	5%
Would you share your account password with another person when needed?	40%	50%	10%
Are you at ease with providing your personal details on internet platforms?	50%	40%	10%
Do you make use of data encryption tools to protect your files and communications?	55%	35%	10%
Are you able to explain what a phishing attack is?	95%	5%	0%
Have you personally received suspicious messages or encountered sites attempting to steal your information?	30%	60%	10%
Do you understand what encryption means and how it functions to protect data?	85%	10%	5%
Do you share cybersecurity knowledge or help educate others about staying safe online?	60%	30%	10%
Are you aware of the steps needed to keep your personal information secure on social media?	65%	25%	10%
Do you turn off location access for applications that have no legitimate need for it?	50%	40%	10%
Have you closed or removed an online account due to worries about its safety or data exposure?	40%	50%	10%

Note: Percentages are based on the total survey sample of N = 150 participants. Responses were originally collected on a four-point Likert scale and subsequently grouped into three interpretive categories (Yes, No, Not Sure) for simplified reporting.

4.2. Qualitative analysis of security behavior

Disaggregating the data by gender, place of residence, and academic discipline surfaces a far more layered story than aggregate figures suggest. Beneath headline awareness numbers lie pronounced sub-group differences, and the consistently observed gap between what students report knowing and how they actually behave turns out to follow predictable structural lines.

4.2.1. Relationship between gender and security behavior

Among the subgroup comparisons, the gender differential is particularly striking. Female students consistently reported stronger adoption of protective security behaviours relative to their male peers — most notably in their more frequent use of robust, non-trivial passwords and their markedly higher rates of two-factor authentication adoption (Figure 1). This pattern is consistent with findings documented elsewhere in the cybersecurity awareness literature, suggesting that female users may be more attuned to personal security risk and more motivated to act on that perception, although the precise mechanisms underlying this behavioural difference remain an open question warranting further inquiry. This finding is consistent with results reported by Alotaibi *et al.* [12] and Johnson and Miller [4], who observed comparable gender-linked differences in security behaviour among university students.

4.3. The effect of academic discipline on security awareness

The breakdown of findings by academic discipline reveals one of the study's most consequential insights. Students enrolled in technical programmes — Computer Science and Networking in particular — not only demonstrated greater conceptual knowledge of cybersecurity but also reported more habitual and

consistent application of protective tools and practices in their daily digital activities (Figure 2). This pattern aligns with findings reported by Al-Janabi and Al-Shourbaji [9] and Kumar *et al*. [11], who similarly found that students in technical disciplines exhibit significantly higher levels of security awareness and practice than their non-technical peers. The most plausible explanation is structural in nature: technical programmes formally integrate cybersecurity content, giving students systematic exposure to the relevant knowledge base and terminology. Students in non-technical disciplines — including arts, social sciences, and humanities — enjoy no equivalent curricular exposure, and the data show that this structural gap produces a real and quantifiable awareness deficit. Addressing this disparity will require deliberate, policy-level institutional decisions; it cannot be assumed that general digital competence provides an adequate substitute for focused security education.

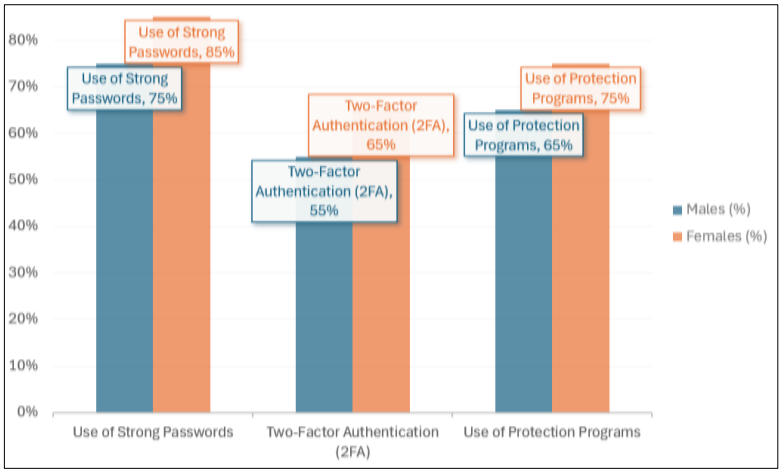

Figure 1. Relationship between gender and security behavior

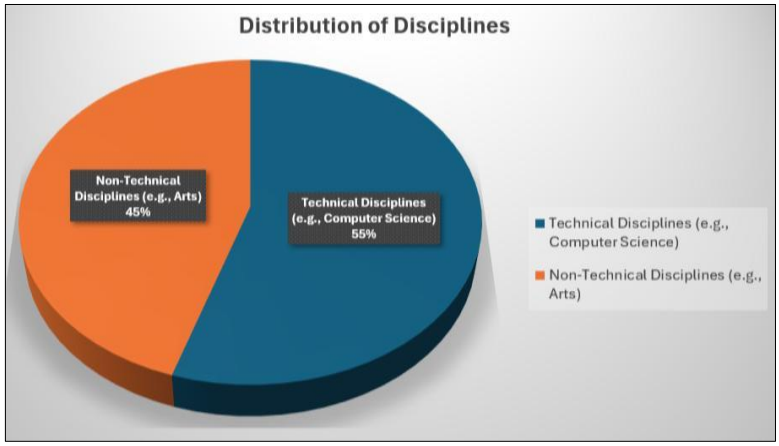

Figure 2. Level of awareness and security practices between students from technical and non-technical disciplines

4.4. Trend analysis in the data

Cognitive awareness — Eighty-five percent of respondents stated that they were familiar with the concept of information security — a figure that speaks to a reasonably widespread baseline of conceptual recognition. However, it is worth being precise about what this figure does and does not tell us. Familiarity with a concept is not the same as competence in applying it. A student who knows what a phishing attack is in the abstract may still click on a convincing phishing link when one arrives in an inbox. What matters is not just whether students have encountered the idea of cybersecurity, but whether they have internalised the habits and judgment that enable them to act on that knowledge under the pressures of real digital life.

Security behavior: the gap that opens between awareness and action is best understood not as a failure of intelligence but as a failure of habit formation. Only 70% of students — 15 percentage points fewer than those claiming conceptual familiarity — reported consistent use of firewalls and antivirus software. This discrepancy is not trivial. It suggests that a substantial number of students occupy an uncomfortable middle ground: aware enough to recognise they should be doing more, but without the practical prompts, skills, or motivation to actually do it. Plausible contributors include uncertainty about how to configure security tools correctly, a generalised sense that attacks happen to other people, and the friction of changing ingrained digital habits.

Behavioral disconnect between awareness and action: examining specific behavioural patterns sharpens the picture further. Students who by their own assessment understood the significance of cybersecurity were simultaneously self-reporting behaviours that any security practitioner would classify as high-risk: constructing passwords for ease of recall rather than robustness; conducting sensitive transactions over unencrypted public networks; and postponing software update installations for weeks or months. The durability of these behaviours in the face of acknowledged risk signals a motivational and practical dimension that purely informational education is unlikely to reach. What is required is an educational approach oriented toward changing what students actually do, not merely expanding what they know.

Security tools usage: a more fine-grained examination of tool usage makes the picture still more concrete. Of the 70% of respondents who reported using antivirus software and firewalls, only 55% adhered to the maintenance routines — regular signature updates, appropriate inbound traffic restrictions — that are necessary for those tools to deliver genuine protection rather than a superficial sense of security. The distinction between installing a security tool and operating it correctly may appear minor, but in practice it separates a genuinely defended system from one that merely presents the appearance of defence while remaining substantially exposed. The educational implication is unambiguous: instruction must move beyond enumerating which tools students should use, and focus on cultivating the habits of active, sustained security management (Figure 3).

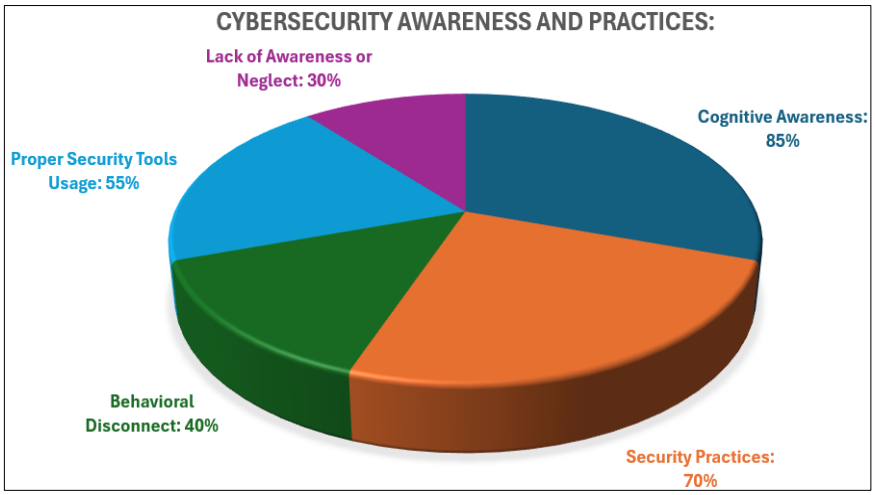

Figure 3. Cybersecurity awareness and practices

4.5. Effects of factors and directions

Gender, academic background, and geographic origin all functioned as reliable differentiators of cybersecurity awareness and security-related behaviour in this dataset. Making sense of how these three dimensions operate — both separately and in interaction — is indispensable for shaping educational responses that are genuinely targeted rather than generic. What follows takes each research question in turn and grounds the analysis squarely in the evidence.

4.6. Research questions

- *Research Question 1: How comprehensively do university students in Jordan understand information security concepts and translate that understanding into practice?*

At first encounter, a reported awareness rate of 85% might seem sufficient cause for optimism. Scrutinised more carefully, it serves better as a prompt for further questioning. Among that 85%, a full 15

percentage points — representing a sizeable cohort — failed to back their stated familiarity with consistent protective behaviour. This suggests that many students have absorbed the terminology of cybersecurity without internalising the practices it demands. Security awareness is perhaps best conceived not as something you either have or lack, but as a graduated scale running from elementary conceptual exposure at one end to deeply ingrained protective habit at the other. Survey respondents tend to cluster in the middle of this scale, precisely where purposeful educational design can achieve the most.

- *Research Question 2: Does a student's gender, field of study, or place of residence have a measurable bearing on how well they understand and apply information security in Jordan?*

Each of the three variables proved meaningful, though the mechanisms differed. Female students outperformed their male peers across most behavioural measures, echoing patterns found repeatedly in the wider literature and suggesting that gender shapes how individuals perceive and respond to personal security risk. The clearest structural explanation applied to the discipline effect: students in technical programmes benefited from embedded cybersecurity instruction, producing both greater knowledge and more consistent tool use, while those in non-technical fields lacked equivalent curricular exposure. This is an institutional outcome, not a reflection of ability, and it has direct implications for course design across all disciplines. Urban location amplified the discipline advantage by granting access to workshops, professional events, and learning resources concentrated in cities such as Irbid that remain less available to students from rural communities. Without deliberate institutional intervention, none of these disparities will diminish.

- *Research Question 3: How do students perceive the importance of information security, and what are the primary challenges they face in applying this knowledge in their daily lives?*

Nine in ten students acknowledged that information security is personally significant to them — arguably the most unambiguous positive in the entire dataset, confirming that the importance of digital self-protection is broadly recognised. The problem lies not in motivation but in execution: converting that principled recognition into consistent daily practice. Students pointed to a familiar set of obstacles: keeping pace with the constantly evolving threat environment is demanding; practices like two-factor authentication and careful password management carry a perceived effort cost; and unclear guidance leaves many unsure where to begin. These difficulties are surmountable with the right institutional support, but they will not dissolve simply because campaigns continue to assert that cybersecurity matters, without engaging with the practical and motivational barriers preventing students from acting on that belief (Figure 4).

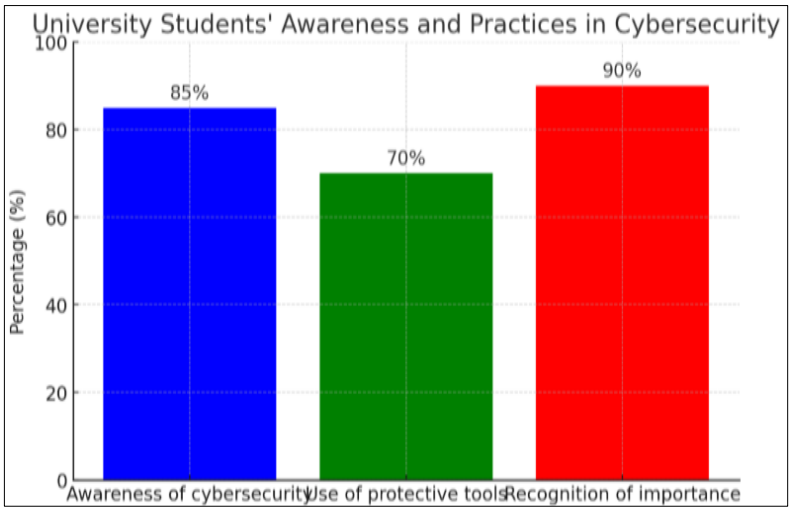

Figure 4. Students' awareness and practices in cybersecurity

5. RECOMMENDATIONS

What the data reveal is not a student population indifferent to cybersecurity but one in which awareness has consistently outpaced practice. Students broadly understand that their digital behaviour carries security implications; fewer have developed the specific, consistent habits that would make that understanding meaningful. The missing element is infrastructure: organised, well-designed pathways through which general awareness is converted into reliable protective action. The recommendations set out below are conceived as the components of precisely that infrastructure.

It is worth noting that the imperative to protect others—not merely oneself—runs through many traditions. In Islamic teaching, the call to collective responsibility for communal wellbeing is explicit: "And cooperate in righteousness and piety, but do not cooperate in sin and aggression." (Surah Al-Mā'idah, 5:2) [25]. Cybersecurity awareness, understood in this light, is not simply a matter of individual self-interest but carries the character of a shared social responsibility [26]-[28]. The following recommendations are proposed:

- R1. Sustain ongoing digital safety campaigns: one-off events and periodic seminars leave little lasting imprint on entrenched digital habits. What is needed are rolling, year-round programmes that position cybersecurity learning as a core institutional obligation, continuously updating students on how the threat landscape is shifting and what concrete protective measures are available to them.
- R2. Embed digital security across all degree programmes: restricting cybersecurity instruction to technical degree programmes means that most graduates enter working life and professional environments lacking even the most elementary digital safety competencies. Weaving security concepts organically into courses across all faculties — rather than creating isolated modules — represents the most sustainable institutional response.
- R3. Deliver hands-on security software training: awareness that security tools exist is only the starting point; competence in selecting, deploying, and maintaining them is what actually reduces risk. Training that walks students through every stage of a tool's lifecycle — from initial setup to routine upkeep — produces durable protective habits that passive information delivery cannot achieve.
- R4. Strengthen applied cybersecurity skill development: drills that replicate real phishing scenarios, structured workshops on constructing unguessable passwords, and guided two-factor authentication activation sessions all exemplify the form of learning that transforms theoretical understanding into ingrained protective habit. Investment in such experiential provision across every faculty is a high-return institutional priority.
- R5. Build recognition skills for phishing and digital fraud: a near-universal recognition of the term "phishing" provides a solid foundation from which to advance. The critical next step is equipping students with the ability to detect live phishing attempts, including the more sophisticated manipulation techniques increasingly directed at social media users, messaging app contacts, and professional networking platforms.
- R6. Encourage robust credential and verification habits: despite being one of the most accessible and highest-impact security practices, strong password management remains far from universal among students. Structured guidance that normalises the use of dedicated password managers and multi-factor verification tools — making them feel routine rather than burdensome — would yield significant protective gains.
- R7. Educate students on public network risks and safe browsing: the genuine hazards of conducting sensitive activities over open, unencrypted networks remain poorly understood by the majority of students. Targeted guidance on the use of virtual private networks, the significance of HTTPS indicators, and the categories of digital activity that should never be performed over public Wi-Fi connections would close a concrete vulnerability identified in the data.
- R8. Strengthen privacy literacy on digital platforms: social media platforms serve simultaneously as students' primary space for self-disclosure and as a major vector for social engineering and identity-based attacks. Programmes that walk students through privacy configuration, data exposure minimisation, and the manipulative techniques used to exploit platform users for phishing and credential theft are overdue.
- R9. Deliver inclusive security education to all disciplines: the security knowledge divide separating students in technical disciplines from those in other fields will not narrow through passive means. Bespoke programmes built specifically around the needs and digital contexts of non-technical students — employing plain language, relatable scenarios, and hands-on exercises — need to be developed, resourced, and mainstreamed across all faculties.
- R10. Foster responsible and secure online conduct: fundamental safe-browsing competencies — including validating software sources before installation, scrutinising link destinations before clicking, and distinguishing trustworthy sites from fraudulent ones — should be conveyed as practical, teachable skills rather than left to students to acquire through trial and error.
- R11. Establish campus-wide device security assistance: a significant proportion of students lack either the technical confidence or the prior experience to secure their own devices and accounts without assistance. A dedicated institutional support service with an explicit mandate to help students configure and maintain their digital security would offer an important resource, especially for those from educationally disadvantaged or rural backgrounds.

- R12. Promote a habit of timely software maintenance: maintaining software currency is among the most consequential and readily teachable security habits for non-specialist users. Universities should reinforce its importance through repeated, clear messaging, and explore whether campus-wide technical policies — such as automated update enforcement on institutional systems — can remove the barriers that prevent students from acting on this knowledge.
- R13. Implement periodic evaluation of student security readiness: in the absence of systematic measurement, institutions have no reliable basis for judging whether their interventions are moving the needle on student security readiness. Scheduled assessments, supplemented by specialist-led seminars and webinars, would provide the evidence base needed to evaluate programme effectiveness and make evidence-informed adjustments.
- R14. Embed security behaviours into everyday digital routines: the aim that should orient all of these efforts is the internalisation of security-conscious thinking as an automatic orientation rather than a deliberate choice — something students bring instinctively to every digital encounter rather than only those that register as obviously threatening. Reaching this goal demands educational experiences rooted in the actual digital contexts and platforms that students navigate daily.

Taken individually, each recommendation addresses a specific and documented gap in student security preparedness. Taken together, they form a mutually reinforcing institutional strategy whose cumulative effect would be to shift students from a posture of passive recognition to one of active, habituated security conduct — which is, ultimately, the only form of cybersecurity literacy that offers real-world protection.

6. CONCLUSION

This investigation began with a question about whether Jordanian university students are genuinely prepared for the cybersecurity demands of contemporary digital life. The data provide a nuanced answer: broadly aware, but unevenly equipped for practice. The majority of students surveyed have encountered the concept of information security and acknowledge its significance; a meaningfully smaller proportion has converted that acknowledgement into the kind of sustained, habitual protective behaviour that makes a tangible difference to their digital safety. The gap between knowing and doing — measured here at 15 percentage points separating conceptual awareness from consistent tool use — is the study's central finding.

Sub-group analysis gave this central finding its structural contours. The performance gap between students in technical programmes — where cybersecurity content is a standard curricular component — and those in non-technical fields was consistent and substantial across all measured indicators. The performance advantage of urban students over their rural counterparts, most plausibly attributable to differential access to educational resources and professional networks, was equally pronounced. These are not random patterns but predictable outcomes of institutional and geographic structures — structures that universities have both the capacity and the responsibility to address.

The practical conclusions that follow are correspondingly concrete. Students in non-technical disciplines require dedicated cybersecurity programmes designed around their specific needs and communicated in accessible, discipline-relevant terms. Students from rural backgrounds require targeted outreach capable of compensating for the resource asymmetries that place them at a structural disadvantage. And all students, regardless of discipline or background, need educational experiences that do more than convey information — experiences that produce lasting behavioural change through simulation, deliberate practice, feedback, and repetition.

More broadly, this study contributes to an expanding body of evidence indicating that cybersecurity awareness should be treated as a core graduate competency rather than the exclusive domain of technical specialists. Every student who enters the workforce without a functional grasp of digital self-protection carries a personal vulnerability — and by extension, so do the organisations and communities they will go on to serve. Universities that take this responsibility seriously, and pursue it through coordinated institutional action, will be generating an impact that extends well beyond the boundaries of the campus. Future research may expand the study to include larger and more representative samples drawn from multiple universities across Jordan, and apply more advanced statistical techniques such as structural equation modelling or regression analysis to further examine the determinants of cybersecurity behaviour among students.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Khader Musbah Ismail Titi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST

The author declares that there is no conflict of interest regarding the publication of this paper.

DATA AVAILABILITY

The data supporting this research were obtained from multiple sources. The dataset used in this study was collected through a structured questionnaire distributed to university students across Jordan. The anonymised survey responses are available from the corresponding author upon reasonable request.

REFERENCES

[1] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *Journal of Information Security and Applications*, vol. 42, pp. 36–45, 2018.
[2] R. Al-Khasawneh, "Digital security in Jordanian universities," *Jordan Journal of Technology*, 2021.
[3] A. Field, Discovering statistics using SPSS. London, UK: SAGE Publications, 2018.
[4] L. Johnson and R. Miller, "Gender differences in cybersecurity awareness," *Cyber Research Journal*, 2020.
[5] M. Al-Qudah et al., "Cyber threats and awareness among university students in Jordan," *Journal of Information Security*, 2021.
[6] A. Hassan et al., "Urban vs. rural digital security awareness," *Middle East Cybersecurity Studies*, 2019.
[7] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. P. Disso, "Cyber security situational awareness for log analysis," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 1–15, 2016.
[8] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts," *in Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 54, no. 4, pp. 230–234, 2010.
[9] S. Al-Janabi and I. Al-Shourbaji, "A study of cybersecurity awareness in educational environments in the Middle East," *Journal of Information Security and Applications*, vol. 28, pp. 1–7, 2016.
[10] E. Kritzinger and S. H. von Solms, "Cyber security for home users: a new way of protection through awareness enforcement," *Computers and Security*, vol. 29, no. 8, pp. 840–847, 2010.
[11] R. Kumar, S. A. Khan, and R. A. Khan, "Cybersecurity awareness among students: a case study of Indian universities," *International Journal of Information Technology*, vol. 10, no. 2, pp. 221–227, 2018.
[12] F. Alotaibi, S. Furnell, and N. Clarke, "Cybersecurity awareness in Saudi Arabia: a survey of internet users," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 1–8, 2019.
[13] M. Alshaikh, S. B. Maynard, and A. Ahmad, "APAT: a model for enhancing employee awareness of cyber threats," *Journal of Information Security and Applications*, vol. 40, pp. 1–12, 2018.
[14] S. Alzahrani, T. Alharbi, and A. Alshehri, "A model for reducing security and privacy risks in big data environments," *Journal of Big Data*, vol. 7, no. 1, pp. 1–18, 2020.
[15] K. M. E. Titi, "Cybersecurity awareness in Saudi Arabia: a systematic literature review," *Conference: 14th International Conference on Education and New Learning Technologies*, 2022, doi: 10.21125/edulearn.2022.1142.
[16] F. Alotaibi, S. Furnell, and N. Clarke, "Cybersecurity awareness in Saudi Arabia: a survey of internet users," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, pp. 1–8, 2017.
[17] F. Aloul, S. Zahidi, and W. El-Hajj, "The need for effective information security awareness in the UAE," *Journal of Information Security*, vol. 3, no. 3, pp. 1–10, 2012.
[18] F. Quader and V. P. Janeja, "Insights into organizational security readiness: lessons learned from cyber-attack case studies," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 638–659, 2021, doi: 10.3390/jcp1040032.
[19] H. Taherdoost, "A critical review on cybersecurity awareness frameworks and training models," *Procedia Computer Science*, vol. 235, pp. 1649–1663, 2024, doi: 10.1016/j.procs.2024.04.156.
[20] M. Alazab and R. Broadhurst, "A capability-based model for cybersecurity awareness," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 1–12, 2016.
[21] M. O. Khaium, S. A. Sifat, S. T. Maliha and M. M. A. Shibly, "Assessing cybersecurity awareness and legal literacy in Bangladesh," 2023 *IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Thiruvananthapuram, India*, 2023, pp. 422-427, doi: 10.1109/WIECON-ECE60392.2023.10456446.

[22] K. E. Khuda, "Cybersecurity awareness in Bangladesh: challenges and recommendations," *International Journal of Computer Science and Network SecuCyber Security-Related Awareness in Bangladesh: Relevant Challenges and Strategies. In: Jahankhani, H. (eds) Cybersecurity Challenges in the Age of AI, Space Communications and Cyborgs. ICGS3 2023. Advanced Sciences and Technologies for Security Applications. Springer, Cham*, 2024, doi: 10.1007/978-3-031-47594-8_14.
[23] M. A. Hossain, M. M. Rahman, and M. S. Islam, "Cybersecurity awareness in Bangladesh: a survey of internet users," *Journal of Information Security*, vol. 9, no. 3, pp. 1–12, 2018.
[24] R. von Solms and J. van Niekerk, "From information security to cybersecurity," *Computers and Security*, vol. 38, pp. 97–102, 2013.
[25] The Noble Qur'an, Surah Al-Mā'idah (Chapter 5), Verse 2, English translation by M. Khan and M. Al-Hilali. Madinah, Saudi Arabia: King Fahd Complex for the Printing of the Holy Qur'an.
[26] F. Alotaibi, D. Roussinov, A. Mohasseb, S. Furnell, and N. Clarke, "Examining cybersecurity awareness among university students: Challenges and future directions," *Computers and Security*, vol. 124, Art. no. 102971, 2023.
[27] L. Hadlington, M. Popovac, H. Janicke, I. Yevseyeva, and K. Jones, "Exploring the role of work commitment and personal values in predicting cybersecurity behaviors in the workplace," *IEEE Access*, vol. 12, pp. 12894–12905, 2024.
[28] A. Nasir, R. A. Arshah, M. R. Ab Hamid, and S. Fahmi, "Determinants of information security policy compliance behavior across higher education institutions: A systematic review," *Journal of Information Security and Applications*, vol. 81, Art. no. 103695, 2024.

BIOGRAPHIES OF AUTHORS

Khader Musbah Ismail Titi holds the position of associate professor and serves as Head of the Cybersecurity Department at Irbid National University in Jordan. His academic formation spans three institutions and two countries: a B.Sc. in Computer Science from Yarmouk University, an M.Sc. in Information Technology awarded with Distinction from the University of Sunderland in the United Kingdom, and a Ph.D. in Computer Information Systems from the Arab Academy for Business and Financial Sciences. Teaching responsibilities have concentrated on cybersecurity, cloud computing, and data encryption, with supervisory involvement in a wide variety of student research projects. Scholarly interests centre on cloud computing, the IoT, network security, and e-Learning. He has contributed to the literature through published research articles and authored books, and holds professional certifications in MCP, Network+, and A+. Workshop facilitation in e-learning and quality assurance has also formed part of his professional activities. He can be contacted at email: drkhmt@gmail.com.