Journal of Management Practices, Humanities and Social Sciences

Vol 10 Issue 2 pp. 296-308

https://doi.org/10.33152/jmphss-10.2.9



ORIGINAL CONTRIBUTION

Digital Security Awareness and Practices in Omani Higher Education: A Qualitative Analysis

Sheikha Al-Buraiki[1]*, Fatma Hassan Abd Elbasset Mourgan[2], Anas Hanendah[3]

[1, 2, 3]Sohar University, Sohar, Sultanate of Oman

[2]Capital University, Helwan, Egypt

Abstract— The rapid pace of digital transformation has reshaped educational environments worldwide, creating new opportunities while posing complex digital security challenges. For higher education students, secure engagement with technology has become a vital competency, particularly in contexts where digital learning, research, and communication are central to academic and professional success. This paper investigates the digital security practices of higher education students in Oman to identify strengths, weaknesses, opportunities, and threats. This qualitative study examined digital awareness and practices through interviews with sixteen students from different higher education institutions. The data collected were analyzed using the SWOT framework. Students' answers about their knowledge, understanding, and digital security practices revealed that they view digital security as protection and a socio-technical practice, show awareness of digital risks, know sources of security awareness, and practice secure password and account protection. However, the weaknesses students described underscore awareness-practice gaps and barriers resulting from limited security knowledge and risk awareness, and low interest, seriousness, perceived importance and convenience, time pressure, and security fatigue. The opportunities provided by the institutions include institutional awareness and guidance, practical and experiential security training, curriculum integration and formal security learning, and early, mandatory, and continuous training. The students' responses to the interview questions underscore digital security threats, including phishing, suspicious links, fake websites, account hacking, compromise and misuse, financial fraud, information theft, data leakage, exposure, and privacy misuse. In conclusion, while students have basic security knowledge, higher education institutions should build a strong security culture and maintain ongoing awareness programs, clear security policies, regular training, and effective reporting mechanisms to strengthen digital security awareness and practices in Omani higher education institutions.

Index Terms— Digital security, Strengths, Weaknesses, Opportunities, Threats

Received: 15 December 2025; **Accepted:** 22 January 2026; **Published:** 24 March 2026



Introduction

Security in the digital realm is not merely a technical issue but has become an integral part of participation in higher education. Students are now learning, doing assignments, communicating, collaborating, storing files, and more, in interconnected digital environments such as learning management systems, email, cloud storage, mobile apps and institutionally managed networks, and are increasingly experimenting with AI-powered tools (Al Ruheili & Al-Buraiki, 2025; S. Al-Buraiki & Al-Ruheili, 2025; S. A. S. Al-Buraiki, 2026; Delcker et al., 2024; Parambil et al., 2024). This means that the student is not only a passive user, but also an important security player who makes daily choices that impact on personal privacy, academic life and institutional security. Studies in Oman and other higher education institutions have identified varying levels of awareness and gaps in practices such as password security, email judgment, secure software practices and handling online threats (Goliath et al.,

*Corresponding Author: saburaiki@su.edu.om

© 2026 The Author(s). All rights reserved.

2024; Kshetri, Hoxha, et al., 2023; Ramalingam et al., 2016). However, research has paid limited attention to how university students understand digital security and how that understanding shapes their everyday practices. This gap is particularly evident in Omani higher education universities and colleges, where students' experiences, perceptions, and actual security practices remain underexplored from a qualitative perspective.

This study seeks to bridge this gap by investigating higher education students' awareness, behaviors, and challenges related to digital security in Oman. Specifically, it explores what knowledge students have and the practices they follow to protect their digital worlds. The current study aims to answer the following research questions:

1. What strengths characterize students' digital security awareness and practices in higher education institutions in Oman?

2. What weaknesses hinder students' ability to maintain effective digital security practices in higher education institutions in Oman?

3. What opportunities exist within higher education institutions to strengthen students' digital security competencies?

4. What threats undermine students' efforts to maintain digital security in digital educational environments?

This study is significant because it will delve into the awareness and actual practices of students' digital world in higher education. It will provide deep understanding of how university students in Oman perceive digital security and how they implement this awareness in everyday practices. Additionally, the study will underscore the sources of digital knowledge students have, the challenges they encounter and the gap between their knowledge, awareness and the actual practices. As for higher education institutions, the findings will most likely help these institutions to develop more effective awareness and support programs among students. The study also aligns with the goals of Oman's Vision 2040 in relation to digital transformations.

The study intends to fulfill the following objectives,

1. To identify the strengths and weaknesses that characterize students' digital security awareness and practices in higher education institutions in Oman.

2. To uncover the opportunities that exist within higher education institutions to strengthen students' digital security competencies.

3. To explore the threats that undermine students' efforts to maintain digital security in digital educational environments.

Literature Review

Digital security is distinct from but complementary to cybersecurity. While cybersecurity addresses threats to institutional networks and infrastructures, digital security emphasizes safeguarding individual data, accounts, and devices from misuse, theft, or hacking (Armas & Taherdoost, 2025; Herbert et al., 2024; Radanliev, 2024). A secure digital culture, therefore, underpins trust in academic institutions, enhances the safe use of e-learning systems, and support sustainable practices in knowledge management and resource utilization. Previous research findings highlight a pressing need for structured educational interventions that not only address immediate technical threats but also embed digital security awareness within broader developmental and ethical frameworks (Adeshola & Oluwajana, 2025; Alobaid, 2025).

In socio-technical context, there is a fairly consistent pattern of good digital security behaviors among students as identified in the literature. Typical examples of secure behaviors that are operationalized in surveys and awareness models include: secure password management, being cautious with emails, updating software, safe web surfing, protecting mobile devices, and awareness of network threats (Bognár & Bottyán, 2024; Jyoti Hazarika, 2025).

Secure learning is not only about infrastructure, encryption, or institutional controls, it is about students' perceptions of risk, habit formation, convenience, and time pressure responses. For instance, Goliath et al. (2024) and Jam et al. (2025) explored the level of awareness of 266 undergraduate and postgraduate students in higher education in South Africa in relation to managing their passwords, emails, social media and mobile devices using a modified Human Aspects of Information Security Questionnaire, revealing uneven levels of resilience among students. This is supported by Bitton et al. (2020), who showed that there was a gap between the security behaviours reported by students and their actual behaviours observed over a long period of time, indicating that students may overestimate their own abilities. Similarly, Diaz et al. (2020) knowledge alone is not sufficient to explain why people are susceptible to phishing attacks, since the actual behaviour of clicking is more complex and involves more than just knowledge, including context, habit, and user judgement. These studies collectively indicate that digital security in higher education should be considered as a behavioral practice in the context of learning routines and not just a set of technical skills (Bitton et al., 2020; Diaz et al., 2020; Goliath et al., 2024).

In the Omani context, Ramalingam et al. (2016) specifically evaluated security awareness among students, academic staff and technical staff across different educational institutions in the country using the Information Security Awareness Identification Model (ISAIM). They collected data via a survey from 173 participants, and the findings revealed a moderate level of basic awareness of security practices particularly in relation to password management and phishing awareness. However, substantial gaps were identified in institutional security policies and standards, and participation in security awareness training. The fundamental structure of student cyber resilience (Goliath et al., 2024) remains largely the same in more recent work in higher education, with similar indicators as main components, such as password management, social media behavior, mobile-device security, and email judgment. The fact that this convergence is present in all the studies is significant, as it indicates that the concept of "good practice" is no longer vague. Instead, it is about behaviors that can be identified: safeguarding credentials, being aware of suspicious communications, avoiding risky downloads and attachments, maintain secure devices, and exercising more caution when using digital platforms (Datta & Krancher, 2024).

However, the literature provides clear evidence that awareness does not necessarily lead to safe behaviours. Evidence from a number of studies indicates the continued existence of an awareness–behavior gap. In their study, Diaz et al. (2020) discovered that students attending universities have a higher rate of clicking on malicious links in live phishing emails, around 59% of the students that opened a phishing email clicked the link. Intriguingly, there were some students who claimed to be knowledgeable about phishing but at the same time were more susceptible to phishing. This is further supported by the latest qualitative research on phishing decision-making, which reveals that people are often quick to respond to emails due to factors like urgency, familiarity, reward, authority, and cognitive shortcuts, as opposed to thorough verification processes (Jayatilaka et al., 2024). Therefore, Chaudhary (2024) states that awareness raising campaigns are ineffective when they assume that the dissemination of information is enough to change behaviour. The study reveals that good security education goes beyond knowledge transfer and highlights the need to focus on motivation and attitudes, as well as the usability of security advice. That is, it is possible for students to learn how to behave safely in the classroom, and yet not apply these skills in real classroom settings (Chaudhary, 2024; Diaz et al., 2020; Jayatilaka et al., 2024).

There are links between students' security practices and their academic level, security training, and academic discipline, but these are not always clear. Goliath et al. (2024) found that postgraduates' digital security awareness and practices are superior in various aspects, suggesting the existence of a "cybersecurity-resilience gap" at an earlier stage in students' education. But the literature cautions that technically oriented students do not necessarily make secure users. When comparing competent digital security and non-competent university students, Kshetri, Hoxha, et al. (2023) highlight that even when the students know about digital threats, they do not do much to protect themselves, but only the basic and easy-to-adopt. The argument is similar to that of Kraus et al. (2023), who argue that IT professionals of the future should be targeted for awareness raising as they are influential digital actors, and they themselves would benefit from more structured and explicit awareness education. The implications of these findings for higher education research are significant, as they call into question the notion that the more digital the more secure. Overconfidence can be as easily brought about by familiarity as it can be by competence Diaz et al. (2020), Goliath et al. (2024), Kraus et al. (2023), and Kshetri, Hoxha, et al. (2023).

One of the other common themes is the security issues that arise in a platform dependent and Bring Your Own Device (BYOD) environment. Higher education is unique in its exposure, as it combines the norms of open access, a large user base, varying levels of technical literacy and a higher level of reliance on personally owned devices (Jimshith & Mary Amala Bai, 2024; Kurnaz & Tekin, 2025). Barrier-free internet access and BYOD policies can pose significant risks for the e-learning infrastructure, particularly when convenience and accessibility are considered without the same level of consideration for authentication, device trust, or network segmentation practices(Tchao et al., 2017). This concern is echoed by the Omani studies conducted by Ramalingam et al. (2016) which revealed a lack of awareness among students, as well as the overall security implementation and training environment in educational institutions. This implies that the responsibility of digital security among students cannot be delegated only to them. A competent user is thus needed along with a well-designed institutional system to establish a secure digital learning environment Ramalingam et al. (2016) and Tchao et al. (2017).

Of the institutional strategies, curriculum integration seems to be particularly promising. Azzeh et al. (2022) studied the integration of digital security concepts in several of the university's courses and found that the pre- and post-test results showed improvement in 11 of 14 digital security topics. This is not a specialist module approach to digital security but rather a cross-cutting approach which can be developed incrementally throughout the curriculum as a literacy. Kraus et al. (2023) present additional evidence from an awareness course for computer science undergraduate students, where students expressed appreciation for the course, learning of new material, and perspective shifts and practical transfer.

Moreover, hands-on, experiential and gamified interventions can be very effective in developing practical security behaviors. Mobile gaming-based educational intervention is found to positively impact the phishing avoidance behavior (Tinubu et al., 2023). The message is that students need more than just warnings; they need multiple chances to recognize, judge and respond in low-stakes, but realistic situations. This is further supported by Kebande (2024) who studied the use of virtual laboratories in cybersecurity distance education and concluded that, both learners and educators, found virtual labs engaging, interactive and effective in enhancing understanding. In addition, the best interventions are likely to be those that relate to students' day-to-day academic and personal lives and involve digital security. Recent studies on phishing and information-security behavior indicate that error is more likely to be the result of haste, habituation, information overload, and information mistrust than ignorance. Even with a basic awareness, the situational and cognitive factors influence email decisions, as demonstrated by Jayatilaka et al. (2024). Objective measures of actual behaviors can reveal different information from self-report (Bitton et al., 2020).

The reviewed studies offer good justification for the current study and at the same time show a research gap. While existing work has provided valuable survey data i.e. Goliath et al. (2024), phishing experiments i.e. Diaz et al. (2020) and Jayatilaka et al. (2024), infrastructure analysis and training evaluations (Khan et al., 2023), the majority of these are not in the Omani context (Bitton et al., 2020; Diaz et al., 2020; Goliath et al., 2024; Jayatilaka et al., 2024) among other studies) and are geared towards general users and/or are based on quantitative measurement only. The relevant studies in Oman have mainly focused on institutional awareness profiles i.e. Ramalingam et al. (2016) instead of rich qualitative accounts of the understandings, practices, negotiations, and constraints of security in contemporary digital learning from the perspective of students. Furthermore, much of the literature at the international level i.e. Diaz et al. (2020), Goliath et al. (2024), and Jayatilaka et al. (2024) tends to isolate the problem in one or more variables, such as passwords, phishing, access to the internet or efficacy of training, and not consider the interaction of strengths, weaknesses, opportunities, and threats in the students' own experiences of university life. Despite growing research on

digital security awareness in higher education, limited attention has been given to understanding how students perceive their digital security practices within the broader institutional and environmental context. Existing studies have primarily measured awareness and behaviors through surveys, providing limited insight into the contextual strengths, weaknesses, opportunities, and threats that shape students' digital security experiences. Therefore, there is a need for a qualitative SWOT analysis that captures these interconnected dimensions and generates evidence to inform institutional policies, digital security education, and Oman's digital transformation agenda (Goliath et al., 2024; Ramalingam et al., 2016).

SWOT Analysis Framework

SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis is an approach that is used for planning and managing strategic work in organizations (Hosen, 2017; Rahman et al., 2021), which was originally introduced in the early 1950s to examine the effectiveness of organizational strategies (Rahman et al., 2021). SWOT analysis is particularly utilized to investigate the internal and external factors that affect the uncertainty of the organizational environment (Adebesin et al., 2024). Thus, building organizational strategies can be achieved by following the SWOT analysis approach (Hosen, 2017). In education, the framework of SWOT analysis is reported to be widely used to inform decision making and strategic planning when considering the perceptions and the capabilities of different contributors (Zhu & Justice Mugenyi, 2015).

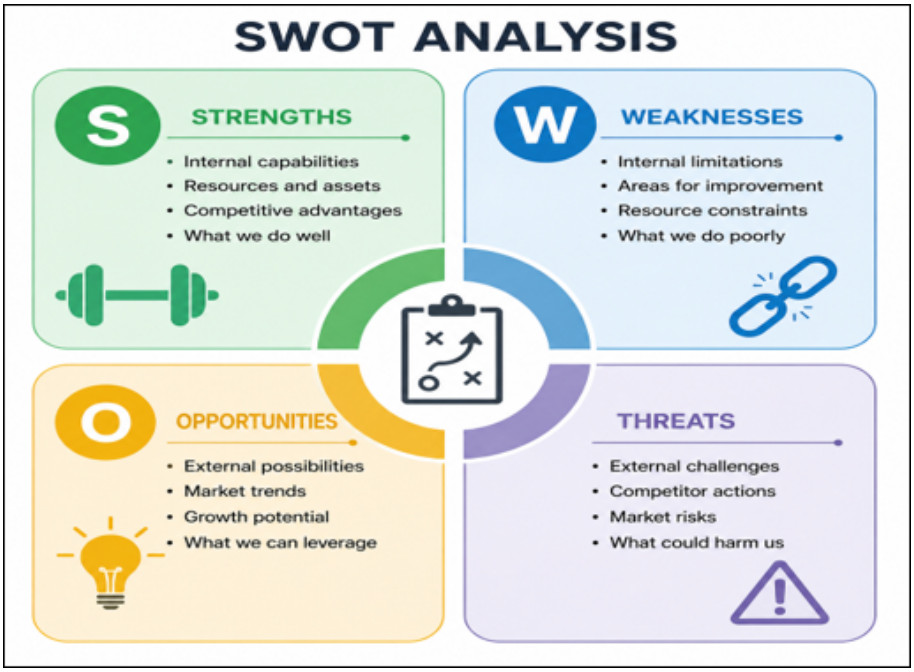


Fig. 1 *A visual representation of the four components of SWOT analysis framework*

The four components of SWOT framework refer to either internal or external considerations. Strengths identify the internal elements that assist the achievement of the organization's goals while weaknesses highlight the internal components that hinder the success of the organization. Opportunities refer to the external aspects of the organization that facilitate achieving its goals in comparison to threats that identify the elements of an organization that represent barriers or potential barriers to the achievement of the organization's goals (Rahman et al., 2021). In any organization, employing SWOT analysis framework benefits the organization's status informing the development of its strategies. Figure 1 shows the four components of the SWOT analysis framework where strengths represent internal capabilities, resources and assets, competitive advantages and what people do well while weaknesses highlight internal limitations, areas for improved performance, resource constraints, and what people do poorly. In comparison, opportunities represent external possibilities, growth potential and what people can leverage while threats underscore external challenges, competitive actions, and what could harm people. Figure 1 has been created using a generative AI tool, ChatGPT.

In the present study, SWOT analysis framework will be adopted to analysis and categorize participants' responses to the interview questions, leading to answering the research questions.

Methodology

Research design

The present study takes a qualitative research approach guided by SWOT as a framework for analysis. Although SWOT analysis is more commonly used to examine organizational environments, in this particular study it has been adapted to organize students' responses that represent their experiences of digital security. Thus, each student is treated as the primary point of reference. Based on this approach, strengths, and weaknesses represent internal factors related to students' knowledge, awareness, attitudes and practices. In the same vein, opportunities, and threats mirror the external factors within the wider digital and institutional environment. A study conducted by Weng et al. (2025) utilized the SWOT analysis framework to explore students' insights into AI empowered entrepreneurship education. Another study conducted by Markos et al. (2024) examined undergraduate students' perceptions of ChatGPT mapping the strengths, weaknesses, opportunities and threats using the SWOT analysis framework. These studies among many others prove that SWOT analysis can be explicitly used to examine students' perceptions and experiences.

Semi-structured interviews were conducted with university level students. The interview questions focused on four areas; questions that uncovered the strengths and weaknesses of digital security knowledge and practices, and questions that explored the opportunities and threats. The interview questions were generated in light of a literature review of pertinent previous studies.

Data collection instrument

The primary data collection instrument was the semi-structured interview. Based on a thorough review of the literature, the interview questions were developed and validated. The interview protocol and questions were validated by a panel of judges who consisted of six university instructors from various disciplines including educational technology, curriculum and instruction, computer sciences and software development. All of the judges hold doctorate degrees and have considerable experience in teaching and research work. They reviewed the interview protocol and questions and provided some suggestions for improvement which included adding follow-up questions and restructuring some other questions for additional clarity. During the interview, the students were asked follow-up questions to seek further information, clarification, or examples. Once the interviews were completed, they were transcribed verbatim using the websites Transcribe and TurboScribe. Following this, the transcripts were checked against the recorded interviews to validate the accuracy of the transcriptions. Some modifications were applied for additional alignment between the two mediums; the audio and transcribed interviews.

Participants

The participants in the study included sixteen undergraduate students who were studying in different higher education institutions in Oman including eight students from Sohar University, two students from Oman Medical College, four students from the University of Technology and Applied sciences, and two students from Middle East College. The students represented different academic disciplines. Specifically, six students were from education, four from information technology, two from engineering, three from computer science, and one from medicine. Their years of studies vary from one student as first year, one from second year, ten from third year and the remaining are in their fourth and last year of study. There were nine female and seven male students. They were approached based on their willingness to participate in online interviews via Microsoft Teams. Their consent was considered and the interviewer illustrated to them that the data derived from the interviews would remain confidential and would be used for research purposes only. The time of each interview ranged from 20 to 40 minutes. All the interviews were carried out in English and were conducted by one of the study researchers and a research assistant. In this research, the participants were assigned pseudonyms to ensure a higher degree of anonymity and confidentiality.

It should be noted here that although the participants represented different academic disciplines and study levels, the purpose of the study was to gain an in-depth understanding of students' digital security experiences. Hence, the research objectives did not involve comparing specific disciplinary or year-level groups. The sample of 16 participants was considered adequate for the qualitative nature of the study, as the interviews provided rich and detailed accounts and recurring patterns became evident across participants. While some differences in individual experiences were observed, no clear patterns related specifically to academic discipline or year of study emerged from the data. Therefore, the findings were interpreted across the sample as a whole rather than as comparisons between subgroups.

Trustworthiness

In qualitative research, researchers rely on trustworthiness to establish the research validity as qualitative work explores human experiences rather than numbers. Trustworthiness can be achieved via credibility of truth, transferability which ensures applicability of research findings, dependability which illustrates consistency and confirmability that refers to neutrality (Ahmed, 2024; Novak & Jen, 2024). With reference to Noble and Smith (2025) and in connection with the present research, trustworthiness was ensured by the following strategies.

1. Neutrality has been achieved by discussing emerging themes with the research team members to reach a consensus. In this process, inter-coder reliability was calculated using the percentage of agreement between the two coders. Their initial coding was compared, resulting in

an overall inter-coder agreement of 93.6%. The remaining 6.4% represented coding disagreements due to misinterpretations of codes. These discrepancies were discussed by the two coders and resolved through consensus after referring back to the original interview data.

2. Credibility has been established using several strategies. First, the semi-structured interviews were audio recorded allowing for iterative process for revisiting the data to check emerging themes. Second, the 16 interviews were coded and analyzed by two members of the research team, achieving an initial inter-coder agreement of 93.6%, with disagreements discussed and resolved through consensus. Finally, rich and thick quotes from participants were used to assist the reader in making judgments about whether the themes are true to participants' accounts and grounded in their actual experiences and perspectives.

3. Applicability of findings was achieved by providing rich detail about the research context and participants which is believed to facilitate transferability to other similar populations.

Researcher reflexivity

The researchers of the paper are academics working in higher education. Therefore, they have experience with the educational and digital context examined in this study. However, the researchers remained aware of how their prior knowledge could influence the interpretation of the data. Therefore, to reduce this influence, the transcriptions of the interviews were revisited throughout the analysis, and coding decisions were discussed between two researchers until agreement was reached. Although some members of the research team had previously conducted SWOT-based research related to artificial intelligence in higher education, the interview questions used in the present study were developed specifically to explore students' digital security awareness and practices and were not adopted from the previous studies.

Qualitative data analysis

Using Atlas.ti 26, the semi-structured interviews were analyzed qualitatively. Table I displays the total quotations that relate to each research question and theme.

Table I
The representation of final themes in the coded interview data

Themes	Total quotations	%	Presentation
RQ1- Theme 1 Strengths	223	31.3	Strongly represented
RQ2 – Theme 2 Weaknesses	165	23.1	Moderately represented
RQ3 – Theme 3 Opportunities	234	32.8	Most represented theme
RQ4 – Theme 4 Threats	91	12.8	Least represented theme
Total	713	100	All coded quotations

The students talked about four themes; strengths representing existing awareness and practices, weaknesses illustrating gap in awareness and practice, opportunities that highlight the institutional support and finally threats that indicate external digital risks. Table I shows that the most frequently represented theme was the one that addressed RQ3 (What opportunities exist within higher education institutions to strengthen students' digital security competencies?), which is the institutional capacity-building for secure and future-read digital learning with 234 quotes referring to it followed by the quotes that align with RQ1(What strengths characterize students' digital security awareness and practices in higher education institutions in Oman?) falling under emerging self-protective digital security awareness and practices with 223 quotes. In the third place came the quotes that address RQ2 (What weaknesses hinder students' ability to maintain effective digital security practices in higher education institutions in Oman?) which underscore the awareness–practice gap in students' digital security behavior while the quotes that match RQ4 (What threats undermine students' efforts to maintain digital security in digital educational environments?), expanding socio-technical threats, appeared 91 times. Figure 2 visually presents the thematic map of the SWOT analysis that illustrates the four main themes and their associated subthemes.

Figure 2 illustrates the thematic map generated from the qualitative data analysis. The four main themes are presented at the center of the map, with their corresponding subthemes branching outward. The figure highlights the relationships between students' strengths, weaknesses, opportunities, and threats regarding digital security, providing a visual overview of the key patterns that emerged from the interview data.

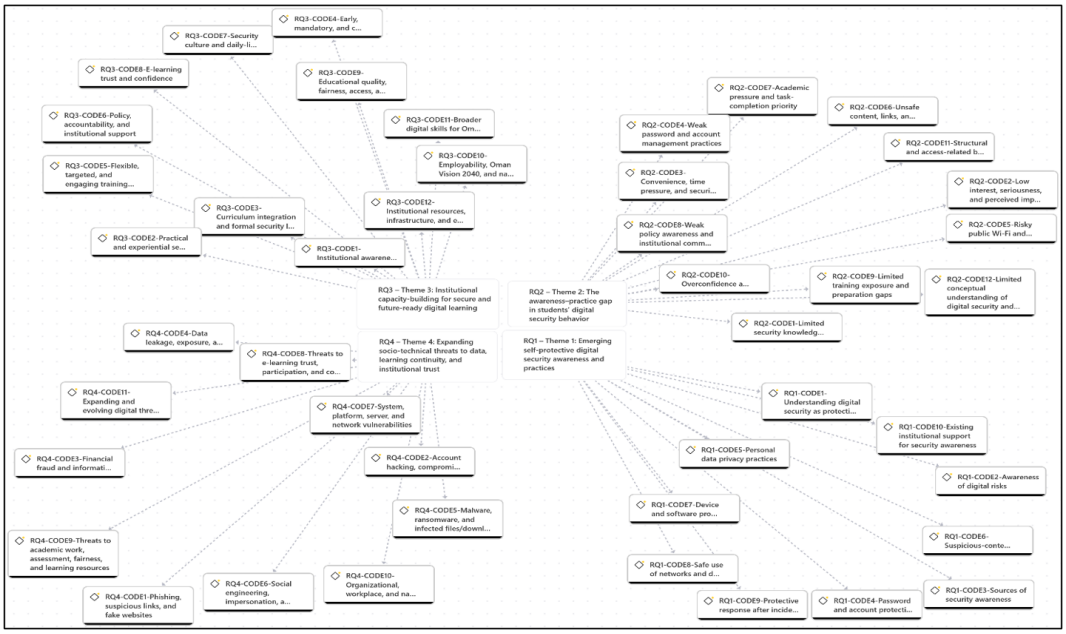


Fig. 2 *Thematic network of students' digital security awareness and practices in higher education*

Figure 3 provides a Sankey visualization of the qualitative findings, demonstrating how participants' responses were distributed across the four themes.

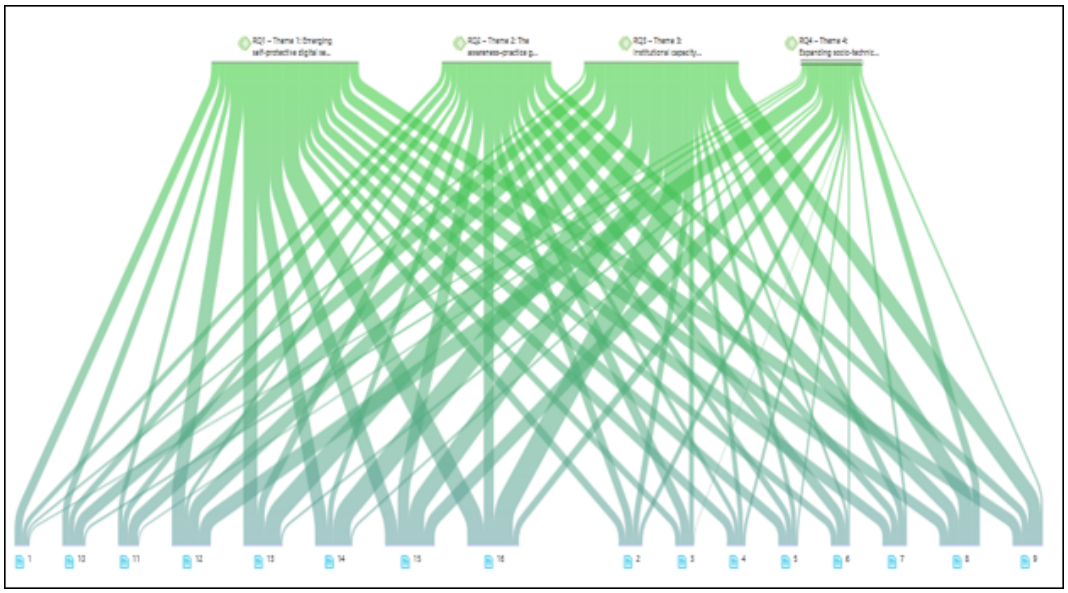


Fig. 3 *Sankey diagram of final themes across interviews*

The Sankey diagram displayed in figure 3 is generated from the qualitative analysis. It illustrates the relationships between the interviewed participants and the four main themes, showing how participants contributed to multiple themes and highlighting the interconnected nature of their experiences with digital security.

In summary, the initial coding process generated 547 in cycle 1 (raw) descriptive codes. These were reviewed, merged, and refined into 45 Cycle 2 focused codes, which were then organized into four Cycle 3 themes aligned with the research questions. The interviews were analyzed using a three- cycle qualitative coding process using Atlas.ti 26. In the first cycle, open coding was employed to identify the meaningful units in the interviews. This stage generated 547 initial codes which reflected ideas related to students' digital security awareness, practices, challenges, opportunities, and threats. Following this, the codes were revised and reviewed. In the second cycle, the initial codes were merged and refined into focused codes. The process resulted in 45 cycle 2 focused codes: Cycle 2 = 45 focused codes (RQ1 – Strengths 10, RQ2 – Weaknesses 12, RQ3 – Opportunities 12, RQ4 – Threats 11). In the third cycle, the 45 focused codes were integrated into four final themes aligned with the

study's research questions and SWOT structure. The final themes are 1. Emerging self-protective digital security awareness and practices, 2. The awareness practice gap in students' digital security behavior, 3. Institutional capacity building for secure and future ready digital learning, and 4. Expanding socio-technical threats to data, learning continuity, and institutional trust. The findings section presents the findings in detail.

Findings

Based on the coding, four main themes emerged. These themes include 1. Emerging self-protective digital security awareness and practices, 2. The awareness-practice gap in students' digital security behavior, 3. Institutional capacity building for secure and future ready digital learning and 4. Expanding socio-technical threats to data, learning continuity, and institutional trust. Each one of the themes provides answer to a research question. A detailed report of findings is provided in the following section.

Theme 1: Emerging self-protective digital security awareness and practices.

The first research question in the present SWOT analysis paper is: What strengths characterize students' digital security awareness and practices in higher education institutions in Oman? The interviewed students demonstrated their awareness of many aspects of digital security. The students' answers to the questions related to their knowledge, understanding, and practices of digital security revealed their

- Understanding digital security as protection and socio-technical practice
- Knowledge about Sources of security awareness
- Secure practices of password and account protection practices
- Awareness of personal data privacy practices
- Management of suspicious-content
- Device and software protection measures
- Safe use of networks and devices
- Protective response after incidents
- Knowledge of existing institutional support for security awareness

For instance, when the students were asked how they define digital security, one of them, Shatha, stated that "being able to use my device and download files and access websites without the fear of getting my information stolen or getting my account hacked". This student understands being digitally secured as a protection and socio-technical practice and is aware of digital risks. When it concerns to secure digital practices, Najat mentioned using "some techniques like having a specific password for every single service, not the same password" while Ameena using "a password manager" depicting personal data privacy practices. Some students follow cautious practices like not sharing their personal private data with random people or websites and logging out of accounts especially when using university computer labs.

From students' responses, it has become clear that they have become aware of the importance of digital security and have implemented a range of protective measures, including privacy protection, strong passwords, avoiding suspicious links, updating devices, using Wi-Fi carefully, and learning from family, schools, universities, social media, and incidents.

Theme 2: The awareness practice gap in students' digital security behavior

The second research question in the present SWOT analysis paper is: What weaknesses hinder students' ability to maintain effective digital security practices in higher education institutions in Oman? Through the interviews, the weaknesses that students explained underscores their awareness and practices gaps and barriers. These weaknesses in students' digital security practices are the results of

- Limited security knowledge and risk awareness
- Low interest, seriousness, and perceived importance
- Convenience, time pressure, and security fatigue
- Weak password and account management practices
- Risky public Wi-Fi and device-use behavior
- Unsafe content, links, and platform behavior
- Academic pressure and task-completion priority
- Weak policy awareness and institutional communication
- Limited training exposure and preparation gaps
- Overconfidence and perceived invulnerability
- Structural and access-related barriers
- Limited conceptual understanding of digital security and educational relevance.

In relation to digital security, students reported several factors that limited their digital security practices. Some participants indicated that security was not always a priority during periods of academic pressure. For instance, Ameena stated that "When students are stressed, for

example, security is not their main focus" illustrating a behaviour that may risk users, particularly students, privacy and secure digital engagement. Bedoor pointed out that based on her knowledge and colleagues relationships, "a lot of students just don't really know enough about it. Also, sometimes it feels like extra effort and people just ignore it". These responses show that students identified academic pressure, limited security knowledge, and low interest as factors that affect their digital security practices.

Theme 3: Institutional capacity building for secure and future ready digital learning

The third research question is: What opportunities exist within higher education institutions to strengthen students' digital security competencies? Analyzing students' responses to the interview questions regarding the opportunities offered and initiated by the institutions revealed the following potential opportunities:

- Institutional awareness and guidance
- Practical and experiential security training
- Curriculum integration and formal security learning
- Early, mandatory, and continuous training
- Flexible, targeted, and engaging training delivery
- Policy, accountability, and institutional support
- Security culture and daily-life relevance
- E-learning trust and confidence
- Educational quality, fairness, access, and academic integrity
- Employability, Oman Vision 2040, and national development
- Broader digital skills for Oman Vision 2040
- Institutional resources, infrastructure, and evaluation support

Students identified several ways in which universities could strengthen digital security among learners. Their suggestions included providing practical training, offering real-life learning experiences, introducing mandatory training from the first year onwards, integrating digital security into the curriculum, and developing clear institutional guidance and policies. Ahmed emphasized that awareness and practical training "should start from the first year and continue every year to remind students." Similarly, Shatha suggested that universities should "include digital security in the curriculum and offer more awareness programs." Sana highlighted the value of experiential learning, stating that "practical workshops and real examples help most students because it's easier to understand when you see real situation." Likewise, Bedoor recommended that universities "should probably organize more workshops and awareness programs. Also, they could include it in courses, so everyone learns it."

Theme 4: Expanding socio-technical threats to data, learning continuity, and institutional trust

The fourth research question is: What threats undermine students' efforts to maintain digital security in digital educational environments? Theme four in the SWOT analysis represents the threats whether they are digital risks or external challenges. Students' responses listed the following threats

- Phishing, suspicious links, and fake websites
- Account hacking, compromise, and misuse
- Financial fraud and information theft
- Data leakage, exposure, and privacy misuse
- Malware, ransomware, and infected files/downloads
- Social engineering, impersonation, and scams
- System, platform, server, and network vulnerabilities
- Threats to e-learning trust, participation, and continuity
- Threats to academic work, assessment, fairness, and learning resources
- Organizational, workplace, and national digital risks
- Expanding and evolving digital threat landscape

Students described a range of digital threats they encounter in educational environments. Their responses highlighted phishing attacks, account hacking, financial fraud, malware, data leakage, platform and network vulnerabilities, risks to academic work and assessment, and threats to trust in e-learning systems and institutional platforms. For example, Nama explained how malware can be distributed through seemingly legitimate files, stating, "I may try now to do a PDF file that has malware or virus and just send it randomly to people that won't know that is actually a malware, not a study file." Similarly, Ayman noted that "if they—students—know the file name, they will just download it without knowing what it is actually inside," describing a common downloading behavior among students. Ahmed also shared his personal experience with malicious software, saying, "Because I downloaded unsafe files, I've been infected with Trojan horses, I've been infected with malware, and the most painful infection was a ransomware that happened to me three times." Ahmed's experience was particularly notable, as he reported

encountering ransomware three times. This was not a common experience among the other participants and can therefore be considered an individual case within the broader theme. Nevertheless, his account highlights the seriousness and potentially recurring nature of the digital threats that some students may encounter.

Discussion

The findings suggest that Omani university students have developed a solid foundation of digital security awareness and engage in a range of self-protective practices, including using strong passwords, safeguarding personal information, avoiding suspicious links, and maintaining updated devices. These findings indicate that students increasingly view digital security as both a technical and behavioral responsibility, reflecting the growing emphasis on individual responsibility in digital environments. This is consistent with previous research, which found that higher education students are generally aware of fundamental digital security practices, particularly those related to password management, phishing awareness, and data protection (Bitton et al., 2020; Ramalingam et al., 2016).

Despite this encouraging level of awareness, the findings also reveal a noticeable gap between what students know and how they behave in practice. Convenience, academic workload, limited training, and overconfidence often lead students to neglect secure practices even when they recognize the associated risks. Similar awareness–behavior gaps have been widely reported in the literature, suggesting that knowledge alone is insufficient to produce lasting changes in digital security behavior. Instead, students require continuous, engaging, and behavior-oriented interventions that strengthen self-efficacy and promote secure habits in everyday digital activities (Chaudhary, 2024; Jayatilaka et al., 2024; Lain et al., 2024). Perhaps more specifically, Lain et al. (2024) demonstrated that the impact of in-person phishing training is often more about the "nudge" of frequent reminders of the risk than users taking the time to learn the material. They also found that when training content is not relevant or there is a lack of time, engagement with the content is decreases. This is especially valuable for students who are frequently subject to time pressure and information overload. It suggests that awareness training should not only be provided by universities but also be made timely, contextualized, repetitive, and in-situ as part of the learning process of the students (Chaudhary, 2024; Lain et al., 2024).

The opportunity theme highlights the important role that higher education institutions can play in strengthening students' digital security competencies. Participants emphasized the need for curriculum integration, practical training, continuous awareness initiatives, and institutional policies that embed digital security into everyday learning. These findings support previous studies advocating a whole-institution approach in which digital security becomes an integral part of teaching, learning, and professional preparation rather than a stand-alone technical topic (Adebesin et al., 2024; Armas & Taherdoost, 2025; Azzeh et al., 2022). Such initiatives are particularly relevant for supporting Oman Vision 2040 and preparing graduates for an increasingly digital workforce.

Finally, the identified threats demonstrate that students operate within an increasingly complex socio-technical environment where phishing attacks, account compromise, malware, data breaches, and social engineering continue to threaten not only personal information but also learning continuity, academic integrity, and institutional trust. These findings reinforce previous evidence that digital security risks extend beyond technical vulnerabilities and require coordinated efforts involving students, educators, and institutions to build a sustainable culture of digital security (Diaz et al., 2020; Goliath et al., 2024; Ramalingam et al., 2016). Thus, moving from diagnosis to intervention, it seems that one-off, optional and purely informational workshops are not sufficient. Explicitly, Ramalingam et al. (2016) mention the absence of awareness programs and training as one of the primary causes of the weakness of the institutions in Oman. Chaudhary (2024) also claims that the majority of the security-awareness campaigns are ineffective due to relying on too general information, fear appeal, or advice that is too out-of-context to be implemented in the real world.

Limitations

This study has several limitations that should be considered when interpreting the findings. Although the present study adopted a qualitative approach to the research design, the small and heterogeneous sample of sixteen students, may render a limitation. In other words, the relatively small and heterogeneous sample may not fully represent the experiences of all higher education students in Oman. A bigger sample size may yield deeper and more complex findings comprehensively reflecting the actual reality. The single-country context will most probably reflect the situation of students' perceptions and practices tightly to a specific higher education context and thus cautions must be exercised when considering other contexts as the findings may not be directly transferable to higher education settings in other countries. Although using SWOT analysis was useful for organizing students' perspectives and experiences into predefined categories of strengths, weaknesses, opportunities and threats, it may have limited the emergence of perspectives that did not fit neatly within these categories. Finally, member checking was not conducted; therefore, participants did not have the opportunity to review and confirm the researchers' interpretations of their responses. However, other strategies were used to enhance the credibility and trustworthiness of the findings.

Implications and conclusion

In light of the findings and in relation to previous pertinent studies, there are several fundamental aspects to elevate and enhance students' digital practices. First, the digital security of students should be considered as a phenomenon of behaviour and institutions and not only as a technical

phenomenon. Second, universities need to be studied not only in terms of the risks that students encounter, but also in terms of how the design of the university, its curricula and training can help to establish a safer environment for digital learning. Thirdly, pedagogical paradigm needs to shift towards active performance instead of passive exposure for secure digital learning. This can be achieved through phishing simulations, case-based learning, scenario analysis, virtual lab, and discipline-specific exercises in the higher education context, which will make cyber risk a tangible and not an abstract concept (Kebande, 2024). Fourthly, curriculum integration can also be a solution for higher education institutions looking for scalable solutions, as it can help to decrease reliance on voluntary attendance. In this regard, Kraus et al. (2023) propose that when durable security learning is integrated, scaffolded and normalized as part of academic development, it is more likely to occur than as an occasional add-on to academic development.

In conclusion, digital security education in higher education should not be isolated from the everyday digital practices through which students encounter security risks. Whether accessing email on mobile devices, downloading files during examinations, clicking links shared in class groups, using shared networks, or navigating between formal and informal digital spaces, students require security education that reflects these real-world experiences. Grounding security education in authentic student practices is more likely to enhance its relevance, encourage sustained secure behaviors, and foster a stronger culture of digital security within higher education.

Conflict of interest

The authors declare that they have no conflict of interest.

Acknowledgement

The authors sincerely thank all the students who participated in this study.

References

Adebesin, F., Adeliyi, T., & Oluwadele, D. (2024). Mapping the knowledge landscape of AI in higher education: A SWOT analysis. *Educational Administration: Theory and Practice*, *30*(5), 9068–9087.

Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. *Journal of Computers in Education*, *12*(4), 1283–1305. https://doi.org/10.1007/s40692-024-00346-7

Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *2*, 100051. https://doi.org/10.1016/j.glmedi.2024.100051

Al Ruheili, H., & Al-Buraiki, S. A. S. (2025). Incorporating AI in educational leadership: Trends and innovations. In *Optimizing research techniques and learning strategies with digital technologies*. IGI Global Scientific Publishing.

Al-Buraiki, S., & Al-Ruheili, H. (2025). A qualitative SWOT analysis study of the integration of AI technologies into higher education institutions in the Sultanate of Oman. *International Journal of Learning, Teaching and Educational Research*, *24*(3), 545–561. https://doi.org/10.26803/ijlter.24.3.26

Al-Buraiki, S. A. S. (2026). Empowering educators for the AI era: Strategies for teacher training and professional development. In *Human-centered approaches to ai-enhanced english language learning and teaching*. IGI Global Scientific Publishing.

Alobaid, A. (2025). A didactical framework for raising awareness of digital multiliteracies among university students: Objectives, expectations and challenges. *Discover Education*, *4*(1), 181. https://doi.org/10.1007/s44217-025-00599-z

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

Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). Adopting the cybersecurity concepts into curriculum the potential effects on students cybersecurity knowledge. *Indonesian Journal of Electrical Engineering and Computer Science*, *25*(3), 1749–1758.

Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2020). Evaluating the information security awareness of smartphone users. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3313831.3376385

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, *14*(6), 588. https://doi.org/10.3390/educsci14060588

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, *142*, 103858. https://doi.org/10.1016/j.cose.2024.103858

Datta, P. M., & Krancher, O. (2024). Cybersecurity end-user compliance: Password management versus update compliance. *Information & Management*, *61*(8), 104060. https://doi.org/10.1016/j.im.2024.104060

Delcker, J., Heil, J., Ifenthaler, D., Seufert, S., & Spirgi, L. (2024). First-year students AI-competence as a predictor for intended and de facto use of AI-tools for supporting learning processes in higher education. *International Journal of Educational Technology in Higher Education*, *21*(1), 18. https://doi.org/10.1186/s41239-024-00452-7

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343

Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in Higher Education. *International Information Security Conference*.

Herbert, F., Becker, S., Buckmann, A., Kowalewski, M., Hielscher, J., Acar, Y., Dürmuth, M., Zou, Y., & Sasse, M. A. (2024). Digital security a question of perspective a large-scale telephone survey with four at-risk user groups. *2024 IEEE Symposium on Security and Privacy (SP)*.

Hosen, M. (2017). SWOT analysis: A theoretical review. *Journal of International Social Research*, *10*, 51. https://doi.org/10.17719/jisr.2017.1832

Jam, F. A., Ali, I., Albishri, N., Mammadov, A., & Mohapatra, A. K. (2025). How does the adoption of digital technologies in supply chain management enhance supply chain performance? A mediated and moderated model. *Technological Forecasting and Social Change*, *219*, 124225.

Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2024). Why people still fall for phishing emails: An empirical investigation into how users make email response decisions. *In Proceedings of the 2024 Symposium on Usable Security (USEC'24). Internet Society*.

Jimshith, V., & Mary Amala Bai, V. (2024). Evaluation of security framework for BYOD device in cloud environment. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *65*(3), 803–814. https://doi.org/10.1080/00051144.2024.2310458

Jyoti Hazarika, H. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria (Online First)*.

Kebande, V. R. (2024). The impact of virtual laboratories on active learning and engagement in cybersecurity distance education.

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Kraus, L., Švábenskỳ, V., Horák, M., Matyás, V., Vykopal, J., & Celeda, P. (2023). Want to raise cybersecurity awareness? Start with future IT professionals. *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1*.

Kshetri, N., Hoxha, D., et al. (2023). KnowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students. *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*.

Kurnaz, S. Ç., & Tekin, Ö. F. (2025). Ai supported early warning systems in smart disaster Management: The case of Kahramanmaraş earthquakes. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *23*(2), 128–139.

Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S. (2024). Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*.

Markos, A., Prentzas, J., & Sidiropoulou, M. (2024). Pre-service teachers' assessment of ChatGPT's utility in higher education: SWOT and content analysis. *Electronics*, *13*(10), 1985. https://doi.org/10.3390/electronics13101985

Noble, H., & Smith, J. (2025). Ensuring validity and reliability in qualitative research. *Evidence Based Nursing*, *28*(4), 206–208. https://doi.org/10.1136/ebnurs-2024-104232

Novak, A. M., & Jen, E. (2024). The editorial word: Trustworthiness. *Journal of Advanced Academics*, *35*(4), 718–728.

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, *7*, 100327. https://doi.org/10.1016/j.caeai.2024.100327

Radanliev, P. (2024). Digital security by design. *Security Journal*, *37*(4), 1640–1679. https://doi.org/10.1057/s41284-024-00435-3

Rahman, M., Mousa, M. M., & Elwalda, A. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights*, *6*(1), 55–73. https://doi.org/10.5038/2640-6489.6.1.1148

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions.

Tchao, E. T., Ansah, R. Y., & Djane, S. D. (2017). Barrier free internet access: Evaluating the cyber security risk posed by the adoption of bring your own devices to e-learning network infrastructure. *International Journal of Computer Applications*, *176*(3), 53–62. https://doi.org/10.5120/ijca2017915581

Tinubu, C. O., Falana, O. J., Oluwumi, E. O., Sodiya, A. S., & Rufai, S. A. (2023). PHISHGEM: A mobile game-based learning for phishing awareness. *Journal of Cyber Security Technology*, *7*(3), 134–153. https://doi.org/10.1080/23742917.2023.2167276

Weng, X., Gu, M. M., Xia, Q., & Chiu, T. K. (2025). SWOT analysis of Al empowered entrepreneurship education: Insights from digital learners in higher education. *Thinking Skills and Creativity*, *56*, 101763. https://doi.org/10.1016/j.tsc.2025.101763

Zhu, C., & Justice Mugenyi, K. (2015). A SWOT analysis of the integration of e-learning at a university in Uganda and a university in Tanzania. *Technology, Pedagogy and Education*, *24*(5), 1–19. https://doi.org/10.1080/1475939X.2015.1093537