Cybersecurity Awareness Among Undergraduate Students in Saudi Arabia: A Quantitative Study

Turky A. Saderaldin[1], Ali Abuabid[2]*
Dept. of Engineering, King Abdulaziz University, Jeddah, Saudi Arabia[1]
Dept. of Information Technology, Saudi Electronic University, Abha, Saudi Arabia[2]

***Abstract*—Cybersecurity awareness has become increasingly important as digital services expand rapidly in Saudi Arabia. This study presents a quantitative assessment of cybersecurity awareness among undergraduate students in Riyadh and Jeddah. A structured questionnaire was administered to 177 students to evaluate awareness across three dimensions: internet usage, information security practices, and social media and smartphone security. Statistical analyses, including descriptive statistics, principal component analysis, regression, and cluster analysis, were applied to identify patterns and influencing factors. The results indicate a moderate overall level of cybersecurity awareness, with stronger adoption of passive security measures such as antivirus software and firewalls, and weaker engagement with proactive practices, including password management, VPN usage, and two-factor authentication. A key finding is the identification of a smartphone-related security gap: students who rely exclusively on smartphones show significantly lower awareness. The study highlights the influence of device usage and institutional context on cybersecurity behavior and provides recommendations to enhance cybersecurity education and awareness initiatives in higher education.**

***Keywords*—Cybersecurity awareness; undergraduate students; smartphone security; Saudi Arabia**

I. Introduction

The digital revolution has transformed nearly every aspect of modern life. Around the world, societies rely more than ever on information and communication technologies (ICT) for work, education, and social interaction. In Saudi Arabia, this shift has been especially rapid. Under Vision 2030, the Kingdom has embraced digital transformation as a foundation for economic diversity and social development. Recent figures from the Communications, Space, and Technology Commission (CST) show that internet penetration has reached almost 99%, with more than half of users spending over seven hours online each day [1]. These numbers reflect a society that is deeply connected and a youth population that is among the heaviest users of digital platforms.

While this connectivity brings many benefits, it also creates risks. Cyber threats such as phishing, identity theft, and malware often succeed not because of weak technology but because of weak human behavior. Studies repeatedly confirm that the human factor is the weakest link in cybersecurity (Huang et al., 2011; Satar & Alarifi, 2022). University students are a significant group in this regard. They use multiple digital services daily, handle sensitive data, and are part of large open networks, which makes them attractive targets for cybercriminals [4].

*Corresponding author.

A growing number of studies in Saudi Arabia have examined cybersecurity awareness, but the results suggest that challenges persist. In [5], the authors found that many users lack even basic awareness of cybercrime. In [5][6], the authors showed that practices such as strong password management remain weak, while [7] highlighted risks linked to social media and browser security. Other researchers have proposed frameworks and models, such as [8], but these are often resource-intensive and not tailored to everyday student use. What is missing from much of this work is a detailed look at undergraduate students in major cities and how their awareness is shaped by the devices they use. This is a critical gap, especially given that smartphones are now the primary way most students go online [9].

Riyadh and Jeddah provide a unique context for addressing this gap. They are the Kingdom's largest cities, home to some of its most important universities, and central to its economic and technological growth. Understanding how students in these cities think about and practice cybersecurity can therefore provide insights that are relevant not only to the academic community but also to national policy. Since 2017, the National Cybersecurity Authority (NCA) has been working to strengthen awareness and resilience at the national level [10], but effective strategies must start with the groups most at risk.

This study takes up that challenge. It investigates cybersecurity awareness among undergraduate students in Riyadh and Jeddah using a structured 46-item questionnaire. Awareness is assessed across three areas: internet usage, information security [3], and social media/smartphone practices. Beyond simple description, the study applies statistical techniques such as principal component analysis, regression, and cluster analysis to reveal deeper patterns. One of the key findings is what we describe as a "smartphone security shortage", the tendency of smartphone-only users to show significantly lower awareness than peers who use multiple devices.

In doing so, the study makes three main contributions. First, it adds new evidence on Saudi undergraduates, a group that has not been studied in depth despite their importance to the Kingdom's digital future. Second, it shows how device type and institutional setting play a role in shaping security behavior factors often overlooked in prior research. Third, it provides practical recommendations that can support universities, policymakers, and students themselves in building stronger cybersecurity practices. In this way, the study aligns closely with Vision 2030 and with the NCA's mandate to strengthen human-centered cybersecurity in Saudi Arabia.

The remainder of this study is organized as follows: Section II reviews related work on cybersecurity awareness in both the Saudi and international contexts, highlighting existing frameworks and research gaps. Section III presents the methodology, including the survey design, sampling strategy, and data analysis techniques. Section IV reports the results of the study, with descriptive statistics, factor analysis, regression models, and cluster analysis. Section V discusses these findings in light of previous research and considers their implications for students, universities, and policymakers. Finally, Section VI concludes the study with recommendations for practice and policy, as well as directions for future research.

II. Literature Analysis

Cybersecurity is widely recognized as a problem that is as much about people as it is about technology. While tools such as antivirus software, firewalls, and encryption are available, they often fail when users neglect basic practices. Simple habits, such as using weak passwords, ignoring updates, or connecting to insecure networks, can enable serious breaches. Researchers frequently point out that the human element is the "weakest link" in cybersecurity, and this weakness is obvious in younger populations who rely heavily on digital tools but often receive little formal training [2], [11]. For university students, the risk is even greater because of their heavy use of digital services and their constant connection to large, open university networks [12] [13].

In Saudi Arabia, awareness of these issues has grown alongside the Kingdom's rapid digital transformation. Several studies have examined cybersecurity awareness among Saudi users [14]. In [5], for instance, the authors found that basic knowledge of cybercrime remained low, while [15] reported weak adoption of best practices such as strong passwords and identity protection. Research focusing specifically on students has also highlighted problems: [7] showed that many university students neglect browser security and social media privacy, exposing themselves to unnecessary risks. Although useful, these studies tend to focus either on broad populations or narrow aspects of security. Frameworks proposed by [8] and [16] push the conversation further, but one is designed mainly for organizational contexts, and the other focuses only on social media threats. Together, they show progress but leave important questions unanswered.

Looking beyond Saudi Arabia, the same concerns appear around the world. Studies in Europe, North America, and Asia consistently show that students underestimate cyber risks, despite being some of the most digitally active groups [17]. They often understand the theory, knowing, for example, that strong passwords are important, but fail to apply this knowledge in practice. In [18] , [19], and [20], the authors found this "knowledge–behavior gap" among Saudi students, which mirrors findings from other regions. Universities have attempted awareness campaigns, but these are usually generic, leaving students without practical guidance on how to change their everyday behaviors.

Another area that has gained attention is device use. For years, cybersecurity studies assumed that most users accessed the internet via desktop or laptop computers. Today, that assumption is outdated. In Saudi Arabia, as elsewhere, smartphones have become the primary way young people connect online. This shift introduces new challenges. Smartphones encourage convenience, saved passwords, app-based logins, and instant connections, often at the cost of security. International reports suggest that smartphone-first users are more vulnerable to phishing and malicious apps [21] [22]. Locally, [18] highlighted the risks Saudi students face from social media attacks, but did not extend the analysis to general security behaviors. This creates space for deeper investigation, particularly into what we describe as the "smartphone security shortage", where students who depend only on smartphones show weaker awareness across multiple areas.

Institutional and policy contexts also shape how students engage with cybersecurity. Some Saudi universities have integrated cybersecurity into their curricula or conducted training sessions, while others have taken little action beyond posting basic awareness posters. As in [8], the authors highlighted that the organizational culture and governance can make a difference: where institutions prioritize security, students are more likely to adopt secure behaviors. On a national level, the establishment of the National Cybersecurity Authority (NCA) in 2017 was a milestone in coordinating policy and awareness efforts [16]. Yet, implementation across universities remains inconsistent, and the extent to which institutional differences shape student awareness has not been thoroughly tested [23].

Taken together, the literature points to several gaps. First, while cybersecurity awareness has been studied in Saudi Arabia, undergraduates in the country's largest cities, Riyadh and Jeddah, have not been examined in depth, despite their importance as educational and technological hubs. Second, the impact of device type, particularly the dominance of smartphones, has not been fully explored. Third, most existing studies provide descriptive findings but do not use advanced statistical techniques to uncover patterns or predictors of awareness. This study addresses these gaps by combining a focused student population with robust statistical methods, aiming to provide insights that are both academically rigorous and practically useful for Saudi Arabia's digital future.

III. Research Approach

This study aims to provide a clear picture of how undergraduate students in Saudi Arabia perceive and apply cybersecurity principles. Because the focus was on measuring awareness levels and identifying patterns across a relatively large group, a quantitative approach was chosen. Quantitative methods enabled the use of structured questions, comparisons across groups, and statistical tools to uncover trends that might not be visible through simple observation.

A. Population and Sampling

The research targeted undergraduate students at two universities: the King Abdulaziz University (KAU) in Jeddah and the Saudi Electronic University (SEU) in Riyadh. These institutions were selected deliberately because they represent different educational settings. KAU is one of the largest and most traditional public universities in the country, while SEU emphasizes online and blended learning. Comparing students

from these environments provided the opportunity to observe how institutional context might influence awareness.

Reaching students directly was not straightforward; therefore, a non-probability sampling method was employed. The survey was distributed through university email lists, QR codes posted on campus, and links shared via social media. A total of 177 valid responses were collected. While the sample is not large enough to represent all undergraduates in Saudi Arabia, it provides a solid basis for statistical analysis. It reflects the perspectives of students in two of the Kingdom's most important cities.

B. Survey Instrument

The primary data collection instrument was a 46-item questionnaire. Its design drew on previous studies of cybersecurity awareness [5]; [7] and it was refined based on feedback from academic colleagues. The questions were grouped into three main areas: Internet usage, including browsing habits, email use, and online purchases. Information security– including password management, antivirus software, firewalls, and VPNs. Social media and smartphone security – Focusing on How Students Manage Apps, Social Accounts, and Mobile Device Protection. Most questions used a five-point Likert scale ranging from "strongly agree" to "strongly disagree", which helped capture how often students engaged in specific practices. A few multiple-choice questions were also included to gather additional details.

C. Reliability and Validity

Before the survey was widely launched, it was tested with a small group of students to ensure that the wording was precise and that the order of questions made sense. Their feedback led to a few minor adjustments. To check the internal consistency of the questionnaire, Cronbach's Alpha was calculated, producing a value of 0.747. In social science research, this is considered an acceptable level of reliability, indicating that the survey items functioned effectively to measure the intended constructs.

D. Data Collection and Ethics

Data collection lasted approximately eight weeks, from late February to late April 2025. Students were invited to participate voluntarily, and every effort was made to protect their privacy. The survey did not collect names, student numbers, or other identifying information. Participants were informed at the start of the questionnaire about the purpose of the research and how their answers would be used. Ethical approval was obtained from the relevant university committees, and informed consent was obtained from all participants before the survey began.

E. Data Analysis

Once the responses were collected, the data were analyzed using SPSS. Descriptive statistics were first calculated to provide an overview of students' responses to individual items. Subsequently, more advanced techniques were employed. Principal component analysis (PCA) helped to identify broader factors underlying student behavior. Correlation and regression analyses were used to examine the relationships between specific practices and overall awareness scores. Finally, a k-means cluster analysis was performed to classify students based on their cybersecurity behaviors. This step provided valuable insights, showing that students are not homogeneous; instead, they fall into distinct categories, ranging from highly aware to very low adopters of security practices.

The primary objective of this analysis was to determine the main effects of device usage and institutional context on student awareness. While demographic interactions - such as the relationship between gender and previous training, or academic year and field of study—could offer additional granularity, they were excluded from the current model to maintain statistical power given the sample size (n=177) and to prioritize the primary 'smartphone security shortage' hypothesis.

IV. Results

A. Demographics and Reliability

A total of 177 undergraduate students completed the survey. Most respondents were between 18 and 25 years old, which aligns with the typical age range of university students in Saudi Arabia. Regarding devices, nearly all students reported owning a smartphone (98%), while 47% used laptops, 38% used desktops, and 35% used tablets. The prominence of smartphones in this group became a key factor in shaping the results.

The survey instrument was tested for reliability, and Cronbach's alpha (0.747) indicated acceptable internal consistency across items. Table I presents the distribution of device usage among surveyed students, with the combination of "Smartphone with Laptop Computer" being the most common, followed by "Smartphone Only" users (see Fig. 1).

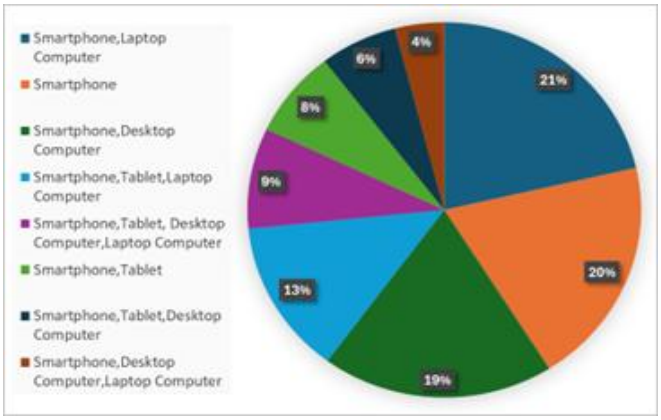

Fig. 1. Comparison of the percentage of device usage combinations.

TABLE I. Device Usage among Undergraduate Students

Device	Number of Students	Percentage
Desktop Computer	67	≃ 38%
Laptop Computer	84	≃ 47%
Smartphone	174	≃ 98%
Tablet	62	≃ 35%

B. General Awareness Levels

Overall, the survey revealed a moderate level of cybersecurity awareness, with an average score of 2.87 out of 4.0 (SD = 0.52). Students reported relatively high use of passive security tools, such as antivirus software (mean = 3.50) and firewalls (mean = 3.04). In contrast, practices that require

ongoing effort, such as maintaining strong passwords (mean = 2.29) or using VPNs regularly (mean = 2.45), were far less common.

Two-factor authentication was adopted by about 40% of participants, which shows some progress but still leaves a majority without this additional layer of protection. The weakest area overall was password complexity, where almost none of the respondents demonstrated high-level practices.

C. Smartphone Security Shortage

The data highlighted a clear "smartphone security shortage". Students who relied exclusively on smartphones scored consistently lower on awareness and secure behavior compared to those using multiple devices. These students were less likely to adopt practices such as two-factor authentication, careful app installation, or frequent updates. By contrast, students who combined smartphone use with laptops or desktops showed stronger security habits across the board.

D. Factor, Correlation, and Regression Analysis

Principal Component Analysis (PCA) grouped the items into three main factors, which together explained 62.3% of the variance:

- Proactive Security Measures – including VPN use, two-factor authentication, and password management.
- Passive Security Tools – such as antivirus, firewalls, and regular updates.
- Smartphone Security Practices – covering app safety and social media security behaviors.

Correlation analysis showed that students who enabled firewalls were also likely to use antivirus software ($r = 0.68$, $p < 0.001$). VPN use was moderately related to two-factor authentication ($r = 0.42$, $p < 0.01$), suggesting that proactive behaviors tend to cluster together. Password complexity, however, remained weakly related to other measures, underscoring its persistence as a challenge.

A multiple linear regression analysis was performed to identify the primary predictors of cybersecurity awareness among students. To ensure the model's integrity and address the reviewer's request for enhanced interpretability, several diagnostic tests were conducted. The Adjusted R^2 was used as a conservative measure of the variance explained by the model, accounting for multiple predictors.

To address the potential for multicollinearity, particularly given the observed correlation between firewall and antivirus use ($r = 0.68$), Variance Inflation Factors (VIF) were monitored. All VIF values remained within acceptable thresholds, confirming that the predictors were sufficiently independent and that the model's coefficients are reliable. The model confirmed that firewall use and two-factor authentication are significant positive predictors of awareness, whereas exclusive smartphone use is a significant negative predictor. This provides robust statistical evidence for the 'smartphone security shortage'. The precision of these estimates was further verified through 95% Confidence Intervals, ensuring that the reported effects are statistically sound.

E. Clusters of Student Behavior

A k-means cluster analysis divided the participants into three distinct groups:

- High Security Adopters (66 students): Regularly used both passive and proactive security measures.
- Moderate Security Users (45 students): Adopted mostly passive tools but were inconsistent with proactive behaviors.
- Low Security Adopters (66 students): Showed limited engagement with cybersecurity practices, with smartphone-only users heavily represented in this group.

Cluster analysis categorized the participants into these groups based on their security behaviors. Specifically, Cluster 3, which consisted primarily of students relying exclusively on smartphones, demonstrated the lowest engagement across all measured awareness dimensions compared to the multi-device clusters. As shown in Table II, this group reported significantly lower rates of VPN usage and manual security configurations ($p < 0.05$).

TABLE II. CLUSTER DISTRIBUTION BY DEVICE CATEGORY

Cluster	Desktop	Laptop	Mobile + Computer	Mobile Only	Multiple Computers
1	31	30	3	12	16
2	8	18	7	17	4
3	6	14	3	6	2

Whereas Fig. 2 illustrates the variation in average scores for Clusters 1, 2, and 3 across survey questions Q3–Q11. Cluster 1 consistently shows higher scores, while Clusters 2 and 3 fluctuate more noticeably, highlighting differences in response patterns and group behaviors.

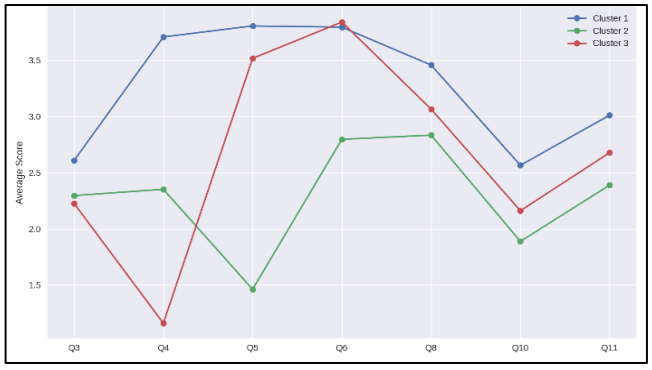

Fig. 2. Average scores across survey questions by cluster.

V. Discussion

The findings of this study reveal a significant discrepancy between 'passive' and 'active' cybersecurity behaviors among Saudi undergraduate students. While the results in Section IV show high adoption rates for antivirus and firewalls, these represent passive security tools that are often automated or pre-installed. In contrast, the lower engagement with active practices, such as VPN usage and multi-factor authentication, suggests that students prioritize convenience over manual

security agency. This behavior indicates that awareness is currently platform-dependent rather than a result of ingrained security habits.

A critical interpretation of the data confirms the identified 'smartphone security shortage'. This phenomenon can be attributed to the 'security abstraction' effect of modern mobile ecosystems. Unlike traditional desktop environments that require frequent user interaction with security prompts and file permissions, smartphones (IOS/Android) are designed to hide these complexities to prioritize user experience. This creates a false sense of inherent safety among exclusive smartphone users, leading to a more passive security posture. Consequently, the 'shortage' identified in this study is not necessarily due to lower intelligence but rather to a lack of exposure to technical security management. This finding is both locally and internationally relevant; global studies have shown that mobile-first users are more exposed to phishing and malware (GSMA, 2022; McAfee, 2023), and in the Saudi context, where smartphone adoption is exceptionally high, this abstraction poses a significant challenge for national cyber-resilience.

The results also show that institutional differences matter. Students from different universities displayed different levels of awareness, suggesting that policies, culture, and training programs at the institutional level can influence student behavior. This finding supports the arguments of [8] and [24], who emphasize the role of governance and organizational culture in promoting cybersecurity awareness. For policymakers and university administrators, this highlights the need for stronger and more consistent cybersecurity initiatives across the higher education sector.

Finally, the cluster analysis underscores that students are not a homogeneous group. Some are highly engaged with both proactive and passive measures, others rely mainly on passive protections, and a substantial group shows minimal engagement. This suggests that awareness campaigns should not take a "one-size-fits-all" approach. Different strategies are needed for different groups: moderate users may benefit from reminders and workshops, while low adopters may require more hands-on interventions. Meanwhile, high adopters could serve as role models or "cyber champions" within their institutions, helping to spread secure habits among peers.

VI. Conclusion

This study set out to evaluate cybersecurity awareness among undergraduate students in Riyadh and Jeddah, two of Saudi Arabia's largest academic and digital hubs. Using a structured survey of 177 students, it assessed practices across internet usage, information security, and social media/smartphone behaviors. The analysis revealed a moderate overall level of awareness, but also significant weaknesses in areas that require active engagement, such as password complexity, VPN use, and consistent adoption of two-factor authentication.

One of the most important findings is what this study terms as the 'smartphone security shortage'. Students who relied exclusively on smartphones consistently showed weaker security behaviors than those who used a mix of devices. Given the central role of smartphones in the daily lives of Saudi youth, this gap poses a serious challenge. The results also show that institutional factors matter: students from different universities reported varying levels of awareness, suggesting that the culture, policies, and training programs within each institution shape student behavior in meaningful ways. Finally, the cluster analysis confirmed that students cannot be treated as a single uniform group; rather, they fall into distinct categories of high, moderate, and low adopters of security practices.

Taken together, these findings carry several implications. At the student level, individuals need to take greater responsibility for their own security. Simple steps—such as creating stronger passwords, enabling two-factor authentication, and using VPNs when accessing public networks—can make a substantial difference. Students should also be encouraged to treat smartphones with the same level of caution as laptops or desktops.

At the institutional level, universities should not rely on generic awareness campaigns alone. Instead, they should integrate cybersecurity education into curricula across disciplines, not just computer science or engineering. Peer-to-peer programs could also be valuable, with highly aware students serving as "cyber champions" who support and influence their peers. Universities with stronger cybersecurity cultures provide a model for others to follow, and there is room to share best practices across the sector.

At the national level, the results align closely with Saudi Arabia's Vision 2030 and the goals of the National Cybersecurity Authority (NCA). Policymakers should recognize the importance of tailoring awareness initiatives to specific groups, such as undergraduates, who represent both current risks and future leaders in the digital economy. National programs could prioritize smartphone security education and promote user-friendly tools that encourage secure habits without creating unnecessary barriers.

Like any study, this research has certain limitations that must be acknowledged. First, the sample was restricted to two universities: the King Abdulaziz University in Jeddah and the Saudi Electronic University in Riyadh. While these institutions represent important academic contexts, the findings are subject to sampling bias and cannot be generalized to all undergraduate students across Saudi Arabia. Expanding the study to include a wider range of universities, technical colleges, and private institutions would provide a more representative picture of student awareness nationwide.

Second, the sample size of 177 participants, although sufficient for the statistical analyses applied, remains relatively modest and was not based on a formal a priori power analysis. A larger dataset would enhance the reliability of factor analysis and regression models, allowing for more sophisticated comparisons across demographic groups. Future research could also employ probability-based sampling techniques to improve external validity and mitigate the limitations of the current convenience sampling approach.

Third, the study relied on self-reported data through a structured questionnaire. While the survey achieved acceptable reliability (Cronbach's $\alpha = 0.747$), self-reports are subject to biases such as social desirability and recall error, which may

lead participants to overestimate their security proficiency. Complementing surveys with behavioral data (e.g., logs of actual password complexity or monitoring of phishing susceptibility through controlled experiments) would give a more accurate assessment of actual cybersecurity practices versus perceived awareness.

Fourth, this study focused on identifying broad trends and did not explore complex interaction effects between demographic variables (e.g., how academic major might moderate the effectiveness of cybersecurity training). Future research utilizing larger, more diverse datasets should employ factorial ANOVA or moderated regression models to investigate these intersections, which would provide a more nuanced understanding of how specific student subgroups respond to security challenges.

Finally, the research design was cross-sectional, capturing a snapshot of student behavior at one point in time. Awareness and practices, however, evolve as new technologies, policies, and threats emerge. Longitudinal studies would allow researchers to track changes over time and evaluate the impact of interventions such as awareness campaigns or curricular integration.

Future studies should therefore broaden the scope geographically, increase sample size, combine self-reported and behavioral measures, and adopt longitudinal or experimental designs. By addressing these limitations, subsequent research can provide deeper and more generalizable insights that support universities, policymakers, and students in strengthening cybersecurity culture in Saudi Arabia.

In conclusion, cybersecurity awareness among Saudi undergraduates is moderate but uneven. Students rely heavily on passive protections while overlooking active security behaviors. The smartphone security shortage is a critical vulnerability that must be addressed urgently. By strengthening awareness at the student, institutional, and national levels, Saudi Arabia can build a more resilient digital society and ensure that its young population is prepared to meet the challenges of an increasingly connected world.

REFERENCES

[1] CST, "Communications, Space, and Technology Commission (CST)."

[2] M. S. Satar and G. Alarifi, "Factors of E-business adoption in small and medium enterprises: evidence from Saudi Arabia," Hum. Behav. Emerg. Technol., vol. 2022, 2022.

[3] D.-L. Huang, P.-L. P. Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information security and their impacts on IT adoption and security practices," Int. J. Hum. Comput. Stud., vol. 69, no. 12, pp. 870–883, 2011.

[4] F. Alharbi et al., "on cyberattack damage: The perspective of small enterprises in Saudi Arabia," Sensors, vol. 21, no. 20, p. 6901, 2021.

[5] M. Almoaigel and A. Abuabid, "Implementation of Cybersecurity Situation Awareness Model in Saudi SMEs," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 11, pp. 1082–1092, Nov. 2023.

[6] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, and J. B. Pickering, "Cybersecurity Awareness and Capacities of SMEs," 2023.

[7] M. Alqahtani, "IOT within the Saudi Healthcare Industry during Covid-19," in Proceedings of International Conference on Emerging Technologies and Intelligent Systems: ICETIS 2021 (Volume 1), Springer, 2022, pp. 469–483.

[8] A. Alshammari, "A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia," Engineering, Technology & Applied Science Research, vol. 13, no. 4, pp. 11445–11450, 2023.

[9] E. S. Mulawwah and H. Almutairi, "Data Security and Cybersecurity in Saudi Arabia," Eurasian Journal of Engineering and Technology www.geniusjournals.org P a g e |, vol. 14, 2023, [Online]. Available: www.geniusjournals.org

[10] National Cybersecurity Authority (NCA), "Policy and Standards," https://nca.gov.sa/en. Accessed: Dec. 04, 2023. [Online]. Available: https://nca.gov.sa/en

[11] D.-L. Huang, P.-L. P. Rau, and G. Salvendy, "Perception of information security," Behaviour & Information Technology, vol. 29, no. 3, pp. 221–232, 2010.

[12] M. Salam, K. A. Abu Bakar, A. T. Abdul Ghani, and A. H. Mohd Aman, "Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities," Sage Open, vol. 16, no. 1, p. 21582440251413470, 2026.

[13] F. Alharbi et al., "The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia," Sensors, vol. 21, no. 20, p. 6901, 2021.

[14] A. Alharbi, H. Mansur, M. Alfuraydan, and T. Atobishi, "Assessing the Determinants of Behavioural Cybersecurity in Healthcare: A Study of Patient Health Application Users in Saudi Arabia," Big Data and Cognitive Computing, vol. 10, no. 2, p. 42, 2026.

[15] M. Hassan, K. Saeedi, H. Almagwashi, and S. Alarifi, "Information Security Risk Awareness Survey of Non-governmental Organization in Saudi Arabia," in The International Research & Innovation Forum, Springer, 2022, pp. 39–71.

[16] Sarah Alghamdi and AbuAbid Ali, "IoT Safeguarding in Saudi Tourism Sector: Crafting a Preliminary Security Model for Enhancing Cyber Resilience," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9, pp. 3847–3859, 2023, doi: 10.17762/ijritcc.v11i9.9641.

[17] A. Bukhatir, M. A. Al-Hawari, S. Aderibigbe, M. Omar, and E. Alotaibi, "Improving student retention in higher education institutions–Exploring the factors influencing employees extra-role behavior," Journal of Open Innovation: Technology, Market, and Complexity, vol. 9, no. 3, p. 100128, 2023.

[18] B. Elnaim and H. Al-Lami, "The current state of phishing attacks against Saudi Arabia university students," International Journal of Computer Applications Technology and Research, vol. 6, no. 1, pp. 42–50, 2023.

[19] Saul Saeed, "Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia," Sustainability, vol. 15, no. 12, 2023.

[20] N. E. M. J. M. G. Wejdan Aljohni, "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 3, 2021.

[21] GSMA, "The Mobile Economy 2022."

[22] McAfee, "McAfee 2023 Consumer Mobile Threat Report," https://www.mcafee.com/blogs/internet-security/mcafee-2023-consumer-mobile-threat-report/.

[23] K. Bwiino, G. K. Mayoka, L. Nkamwesiga, and M. Nyamadi, "A Systematic Literature Review of Information Security Practices in Higher Education Contexts," IET Inf. Secur., vol. 2026, no. 1, p. 6324508, 2026.

[24] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing mitre att&ck risk using a cyber-security culture framework," Sensors, vol. 21, no. 9, p. 3267, 2021.