Global Journal of Information Technology: Emerging Technologies

Volume 15, Issue 1, (2025) 47-63

www.gjit.eu

Cybersecurity awareness among female students at Taif University's faculty of computing and information technology

Nadia Alzaidi [a1], Taif University, Taif, Saudi Arabia, nanana947@gmail.com

Suggested Citation:

Alzaidi, N. (2025). Cybersecurity awareness among female students at Taif University's faculty of computing and information technology. *Global Journal of Information Technology: Emerging Technologies, 15*(1), 47-63. https://doi.org/10.18844/gjit.v15i1.9722

Received from; November 21, 2024, revised from; January 13, 2025 and accepted from March 19.

Selection and peer review under the responsibility of Assoc. Prof. Dr. Ezgi Pelin YILDIZ, Kafkas University, Turkey

iThenticate Similarity Rate: 2%

Abstract

This study investigates the level of student awareness regarding cybersecurity concepts and the methods for achieving cybersecurity within a higher education context. While cybersecurity is a critical component of modern digital literacy, there remains a need to assess how well students comprehend both its foundational concepts and practical applications. This study addresses this gap by examining variations in awareness based on academic degree, specialization, and year of study. A descriptive survey design was employed, and data were collected using a structured questionnaire consisting of two domains. The sample comprised 382 students from a college of computers and information technology. The results revealed a high level of awareness of both cybersecurity concepts and strategies for implementation. Statistically significant differences were identified based on academic degree, with higher awareness among female bachelor's students. Differences were also observed across specializations, favoring students in computer science, information technology, and computer engineering. Additionally, academic year influenced awareness levels, with higher levels reported in the first, third, fourth, and fifth years. The findings emphasize the importance of tailoring cybersecurity education to student demographics and suggest areas for curricular enhancement.

***Keywords*:** Awareness; cybersecurity; digital literacy; higher education; student learning

* ADDRESS FOR CORRESPONDENCE: Nadia Alzaidi, Affiliation, Taif University, Taif, Saudi Arabia
E-mail address: nanana947@gmail.com

1. INTRODUCTION

This era is characterized by rapid technological advancement and the digital revolution in information and communication technology, requiring individuals and institutions alike to adapt in order to both harness its benefits and mitigate associated risks. Among the unintended consequences of these advancements is the emergence of cybercrime, facilitated by widespread internet connectivity and digital interdependence. Modern cyber threats, such as denial-of-service attacks, data breaches, and malware intrusions, pose significant risks to individuals and organizations (Rege & Mbah, 2018). These threats are often exacerbated by the degree to which end users adhere to privacy and security best practices (Howell et al., 2024; Panteli et al., 2025).

Cybersecurity has consequently emerged as a critical discipline aimed at reducing vulnerabilities, preventing security breaches, and enhancing institutional and individual resilience against cyberattacks (Corallo et al., 2022). Effective cybersecurity involves continuous monitoring of systems, identification of vulnerabilities, and implementation of remediation strategies (Raimundo & Rosário, 2022). Alqahtani and Kavakli-Thorne (2023) emphasized the importance of incorporating behavioral change strategies into cybersecurity education to improve its efficacy. Patel (2021) further argued that cybersecurity must be a shared societal responsibility, requiring collective engagement in the application of controls and adherence to protocols designed to protect systems, data, and digital infrastructure.

In light of these realities, there is a growing imperative to implement comprehensive protection measures across all societal sectors. This includes raising public awareness, enhancing cyber-related knowledge, and developing practical skills to foster a secure and resilient digital environment (Khan et al., 2025). Johnson (2022), Adeshola & Oluwajana (2024) highlight that limited awareness of online threats among internet users underscores the urgent need for structured cybersecurity education programs.

In response to growing cyber threats, the Kingdom of Saudi Arabia established the National Cybersecurity Authority (NCA) on November 1, 2017, including the National Cybersecurity Guidance Center as part of its mission to raise awareness among societal institutions and the general public. The NCA's mandate encompasses issuing periodic vulnerability alerts, strengthening local and international partnerships, and disseminating best practices related to digital safety (National Cybersecurity Authority, 2018).

In alignment with these efforts, several initiatives have been launched to promote cyber skills development, such as the @Hack Conference, a premier technical cybersecurity event that provides a platform for knowledge exchange, competitions, and problem-solving activities (Sabq Newspaper, 2021). Among the most impactful training tools are cybersecurity competitions like *Capture the Flag (CTF)* and *King of the Hill (KOTH)*. These competitions offer immersive, gamified environments where students apply both offensive and defensive strategies to tackle real-world cybersecurity challenges (Kucek & Leitner, 2020; Leune & Petrilli, 2017). According to Bock et al. (2018), such events significantly enhance student skills in identifying and mitigating cyber threats while fostering critical thinking and team collaboration.

Moreover, various studies have underscored the value of promoting cybersecurity awareness through creative approaches. Alshahrani and Felemban (2020) recommend that students be encouraged to design educational games aimed at internalizing cybersecurity concepts. Others advocate for educational interventions that address societal risks associated with cyber warfare, legal and ethical responsibilities in digital spaces, and strategies for ensuring personal safety online (Goran, 2017; Mohammed, 2020).

Universities in Saudi Arabia have played a pivotal role in this effort by organizing cybersecurity-focused events and establishing specialized academic programs and digital libraries centered on information security and cybercrime (AlKhodari & Kleibi, 2020). These initiatives serve not only to enhance students' knowledge and preparedness but also to cultivate a broader sense of social responsibility in mitigating cybersecurity risks.

Despite the growing importance of cybersecurity education, there remains a noticeable gap in the literature, particularly within the Arab academic context. A review of current research reveals a scarcity of studies focused on assessing the level of cybersecurity awareness among university students. This gap

underscores the need for further empirical investigation to determine the extent of student knowledge, awareness, and practical competency in the field.

Accordingly, this study aims to explore the following research questions:

RQ1: What level of awareness do students at Taif University's Faculty of Computing and Information Technology have regarding cybersecurity concepts?

RQ2: What level of awareness do students in the Faculty of Computing and Information Technology at Taif University have regarding methods and tactics for achieving cybersecurity?

RQ3: Are there statistically significant differences ($\alpha \leq 0.05$) among the average response of study sample members regarding awareness of methods for achieving cybersecurity based on variables (degree, specialization, academic year)?

The significance of the study is evident in both theoretical and applied dimensions. Theoretically, the study is expected to contribute to the advancement of scientific knowledge by enriching the limited body of Arabic-language research in the field of cybersecurity. It serves as a foundation for future scholarly efforts and aligns with national initiatives aimed at enhancing cybersecurity awareness, particularly within the framework of Saudi Arabia's Vision 2030.

Practically, the study is anticipated to support curriculum developers in emphasizing the importance of integrating practical training related to cybersecurity strategies and techniques. The findings aim to inform university administrators about the need to establish recurring training programs for female students at Taif University. These efforts are intended to promote the development of cyber club initiatives specifically designed to engage and empower this demographic.

The objective of the study was limited to measuring the level of awareness regarding cybersecurity concepts and methods among female students at Taif University. The study was geographically restricted to Taif University and temporally confined to the academic year 2022. Cybersecurity refers to a collection of technologies, processes, and practices aimed at protecting networks, computing systems, software, and data from potential threats, including attacks, damage, or unauthorized access (Rai et al., 2019). Cyber-attacks involve deliberate attempts by malicious actors to inflict damage or destruction on network infrastructures or computing systems (Abu et al., 2018).

1.1. Theoretical framework

1.1.1. Cybersecurity

Universities in Saudi Arabia manage substantial volumes of sensitive data, positioning the nation among those requiring the development of a robust cybersecurity culture to safeguard systems and networks, enhance user trust, and ensure the protection and accessibility of data for timely reference (Albishi, 2021). A significant milestone has been achieved in this domain, with Saudi Arabia ranked second among 153 countries in the Global Cybersecurity Index 2020, as reported by the United Nations agency specializing in information and communication technology (Global Cybersecurity Index, 2020). This accomplishment establishes Saudi Arabia as a model for Middle Eastern and Asian nations seeking to elevate cybersecurity standards.

1.1.2. Cybersecurity objectives

Cybersecurity aims to protect everything related to state and individual electronic activities, from electronic systems and IT networks, all the way down through hardware, software, and equipment affecting services and data storage. This is achieved by creating an infrastructure that safeguards citizens' information, encouraging the application of cybersecurity technologies, and protecting information communication networks that play a vital role in data exchange between peoples - just to name a few additions, electronic transactions are encrypted to protect them against hacks or attacks (Alsayegh, 2018).

It is essential to make users aware of the risks they can encounter through online activities and foster a culture of digital security so they are well-informed on methods for protecting their information and devices

(Kovacs, 2018). as stated in Kolenko (2019) being familiar with cultural and behavioral aspects of cyber-attacks increases individual awareness about cybersecurity while providing requirements to reduce risks against users and remove vulnerabilities in computer systems and mobile devices by instructing individuals on modern mechanisms and procedures (Jaballah, 2022).

1.1.3. Cybersecurity techniques

Institutional practices for strengthening cybersecurity have evolved in line with the growing need for strong protections that shield their systems and data from any incidents, whether accidental or deliberate. Two-factor authentication, also known as two-step verification, has become one of the most essential technologies used to achieve this objective; experts suggest activating two-factor authentication on devices and websites to protect users from hackers or any type of cyber-attack (Qiu et al., 2019). Even with the most advanced and efficient cybersecurity technologies, organizations remain vulnerable to security breaches due to a lack of awareness among users about security procedures and skill sets. According to Moallem (2019), students are not fully informed on how to protect their data, with the two-factor authentication usage rate extremely low; universities should therefore increase awareness regarding two-factor authentication technology's importance in safeguarding devices against cyberattacks. Alqahtani (2022) points out the importance of using antivirus and firewall programs, encrypting important files before sharing them with others, backing up files, and updating programs periodically, which will protect data and devices from cyber breaches.

Cybersecurity techniques should also be applied more carefully and efficiently, with an emphasis on password management. This includes selecting strong passwords that are difficult to guess, changing them periodically, not linking passwords to multiple accounts on websites or social media applications (Aldhawifri, 2021), and not sharing verification codes sent via mobile with others (Gelernter, et al., 2017). as stated in study Muniandy et al., (2017) that revealed a lack of awareness among regarding methods and tactics for protecting from cyberattacks among higher education students in Malaysia, especially regarding phishing attacks, malware, password use, and linking multiple websites. They recommended that cyberspace users receive education on effective strategies to safeguard themselves against attacks, to create an atmosphere of safety online.

1.1.4. Types of cyberattacks

When a device connects to the Internet and initiates communication with external systems, it becomes exposed to a range of risks and threats, both intentional and unintentional. Cyber-attacks manifest in various forms, including malware, which consists of files or programs intended to damage computing systems. These include worms, computer viruses, Trojans, and spyware (Graham et al., 2016). Phishing attacks utilize fraudulent emails designed to resemble legitimate sources to extract sensitive information such as credit card details or login credentials. Findings by Olsen and Tokerud (2020) revealed a significant gap in information security awareness among educators, emphasizing the need for targeted training programs due to widespread unfamiliarity with phishing techniques.

Social engineering attacks exploit human interaction to manipulate individuals into violating security protocols and disclosing confidential information (Sabbagh, 2021). A study conducted by Alsulami et al. (2021) evaluated awareness of social engineering threats within the Saudi Arabian educational sector by surveying students, teachers, and administrative staff. Results demonstrated considerable differences in security practices and competencies between individuals with prior knowledge of social engineering and those without. These findings underscore the necessity for educational institutions to implement customized training initiatives focused on social engineering strategies and broader information security practices, tailored to various age demographics.

The diversity of cyber-attack methods employed by malicious actors highlights the urgent need for institutional action. Organizations of all sizes must adopt proactive measures to secure networks and systems, collaborate with cybersecurity professionals, and prioritize awareness initiatives to educate personnel on potential cyber threats.

1.1.5. Protection against cyber-attacks

Cybersecurity professionals constantly identify and deter emerging cyber threats by developing programs to protect users. To guarantee user protection from the most recent risks, companies must update their programs frequently, Furthermore, users must install antivirus programs that detect and eliminate threats, as well as regularly upgrade both programs and operating systems (Kaur et al., 2021). According to Garba et al. (2020), students lack awareness about password management, phishing attacks, and two-factor authentication procedures, as well as lack effective programs that assess student cybersecurity levels.

Emphasis is placed on cultivating a cybersecurity culture across all segments of society through seminars and various media platforms that educate individuals on methods for protecting personal privacy, particularly given the widespread use of smartphones (Altwairqi et al., 2019). In this regard, Amin et al. (2021) conducted a study to assess the level of security and privacy awareness among smartphone users in Indonesia. The findings revealed a general lack of awareness regarding information security and privacy practices on mobile devices. Similarly, a study by Ahmad Hamed Alsahfy and Saleh Askol (2019) identified significant weaknesses and deficiencies in cybersecurity knowledge among computer science educators.

Alqahtani (2019) investigated the level of cybersecurity awareness among university students in Saudi Arabia by examining perceptions of cybersecurity, common cybercrimes, methods for community-level crime prevention, and social barriers to effective prevention. The study concluded that, while social challenges persist in addressing cybercrime prevention, a major barrier is the rapid progression of information and communication technologies, which are often used by individuals without adequate awareness of associated risks or appropriate mitigation strategies.

The presented findings highlight the critical importance of adhering to preventive procedures against cyber threats, including cautious handling of email attachments from unknown sources. Ndibwile et al. (2019) observed a decline in cybersecurity competence among users who engaged in risky behaviors such as opening suspicious email attachments. Dam (2020) further noted that individuals using unsecured public wireless networks are particularly vulnerable to cybersecurity threats.

Based on these findings, Alqahtani (2019) proposed several key recommendations: enhancing public awareness, strengthening national cybersecurity infrastructure, imposing stricter penalties for cyber-related crimes, and integrating cybersecurity education into academic curricula at multiple educational levels.

1.1.6. Educational institutions' role in promoting cybersecurity education

Educating future generations about the significance of cybersecurity remains a fundamental priority, particularly in the context of rapid technological advancement and the ongoing information revolution that impacts daily life. Cybersecurity also constitutes a core component of the digital transformation agenda and supports the Kingdom of Saudi Arabia's Vision 2030, which aims to develop national capabilities in digital transformation, encompassing email security, data and information protection, and mobile device security (Nasser Mohamed Alshahrani and Felemban, 2020). Key practices include encrypting sensitive files before sharing and employing antivirus software to safeguard data and devices from breaches (Christen, 2020).

The Ministry of Education has emphasized the urgency of enhancing cybersecurity awareness within the education sector. In the current digital era, cybersecurity serves as a critical tool for sustaining societal functions and defending institutions against cyber threats. Therefore, a gradual educational approach is required, beginning with foundational instruction in schools and progressing through higher education institutions (Ministry of Education, 2020).

Several studies have examined the level of cybersecurity awareness among students. Ashafee et al. (2018) researched to evaluate security awareness, preparedness for cyberattacks, and behavioral practices among graduate students in information technology programs. Findings indicated that students in IT fields exhibited significantly higher awareness and more secure behaviors than non-IT professionals. However, the necessity

of enhancing preparedness among both IT and non-IT groups remains evident to mitigate present and emerging security threats. In a related study, Khalid et al. (2018) assessed cybersecurity awareness among students at the College of Education in a Malaysian university using a descriptive survey methodology. While high levels of awareness were observed regarding cyberbullying, personal data protection, and online banking security, notable deficiencies remained in recognizing unethical websites and adopting self-protection strategies.

Tibi et al. (2019) found a substantial decline in both cybersecurity awareness and self-protective capacity among computer science students. The study recommended that higher education institutions offer dedicated training courses to improve responsiveness to cyber threats. Mai and Tick (2021) observed similarly low levels of cybersecurity awareness among university students across academic disciplines and year levels, resulting in limited protection against potential threats. Alkhathami (2020) stressed the importance of integrating information security content into academic curricula to equip students with the skills necessary for countering cyber threats and managing data security challenges.

Institutions of education must actively promote cybersecurity awareness among staff through preliminary seminars, highlighting the risks posed by insufficient knowledge of digital security. Engagement with cybersecurity professionals across sectors is advised to provide comprehensive instruction to educators, enabling them to transfer this knowledge to students. This approach was supported by the findings of Olsen and Tokerud (2020), who documented widespread lack of cybersecurity awareness among teachers. Similarly, Nyinkeu et al. (2018) investigated teachers' knowledge, awareness, and practices related to information security. The study revealed limited understanding of key concepts such as phishing and poor password hygiene, along with misconceptions regarding student capabilities in teaching cybersecurity. Recommendations included the incorporation of cybersecurity education into teacher training curricula, the reinforcement of institutional cybersecurity policies, and the integration of risk analysis and social responsibility components into classroom instruction.

Almuntashari (2020) outlined several strategic recommendations, including the organization of training sessions and workshops on cybersecurity risks and violations in collaboration with the Ministry of Education and national regulatory bodies such as the National Cybersecurity Authority. These initiatives aim to raise awareness among educators in the field. Kritzinger (2017) further affirmed the effectiveness of such interventions, reporting increased teacher awareness following participation in cybersecurity-related training programs.

1.1.7. The role of security in Saudi Universities

The cybersecurity sector in the Kingdom of Saudi Arabia actively contributes to the realization of Vision 2030 by delivering comprehensive awareness and advisory services to individuals and institutions. These initiatives include raising public awareness regarding the protection of personal and national information, providing specialized consultancy services to academic institutions, organizing workshops and conferences focused on digital security, identifying vulnerabilities in digital systems, developing secure responses to breaches, and facilitating the registration of intellectual property through patent protection mechanisms (Alkhodari and Kleibi, 2020).

In alignment with national priorities that position cybersecurity as a cornerstone of secure digital infrastructure, Saudi universities have integrated cybersecurity-related content into their academic offerings. Educational efforts now encompass courses on encryption and information security, the establishment of postgraduate programs dedicated to cybersecurity, and the promotion of student engagement through clubs such as the Cybersecurity Club, Technology and Programming Club, and the Student Developer Clubs Program sponsored by Google. Kritzinger (2017) highlighted the limited awareness of cybersecurity issues among South African students, attributing this deficiency to the lack of comprehensive course content addressing digital threats and protective strategies. This underscores the broader global need for academic institutions to embed cybersecurity education within their curricula.

In recognition of the essential role of cybersecurity in defending against digital threats, several studies have been conducted to evaluate the current status of cybersecurity within higher education institutions. Alshawabkeh (2019) reported that Taif University had implemented strong information security measures designed to mitigate risks and prevent network intrusions. In contrast, Almanea (2022) found that cybersecurity infrastructure within Saudi universities remains insufficient to meet the strategic expectations of Vision 2030, identifying systemic weaknesses that hinder optimal protection. Further examination by Faraj (2022) explored faculty motivations for supporting cybersecurity initiatives at Prince Sattam bin Abdulaziz University. The findings emphasized the influence of social responsibility and public awareness as primary motivators for improving cybersecurity culture. Although technical justifications were acknowledged, they were found to be only moderately compelling, indicating a need to further enhance digital competencies and infrastructure in alignment with national goals.

1.1. Purpose of study

This study sought to identify the level of awareness among students at the Faculty of Computing and Information Technology regarding cybersecurity concepts, determine their level of familiarity with methods for attaining cybersecurity, and uncover any differences in response rates among study sample members on these matters (degree, specialization, academic year).

2. METHOD AND MATERIALS

The survey descriptive Methodology was used as the appropriate Methodology for this study. The questionnaire was used as a means of data collection.

2.1. Participants

The study population consisted of all female students of the Faculty of Computing and Information Technology at Taif University for the current academic year (2021/ 2022). The study sample was selected randomly, consisting of 382 students from the Faculty of Computing and Information Technology at Taif University. The following tables display the distribution of this sample according to various study variables.

Table 1

Distribution of the study sample according to the degree variable

Degree	**Diploma**	**Bachelor's**	**Total**
Frequency	92	290	382
Percentage	24.1%	75.9%	100%

Table (1) shows that those who have a diploma were (92) by (24.1%) and those who have a bachelor's are (290 by (75.9%), respectively. These numbers are representative of the study population.

Table 2

Distribution of the study sample according to the specialization variable

Specialization	Computer Maintenance	Programming Technology	Network Technology and Security	*CS	**IT	***CE	Total
Frequency	31	27	34	95	91	104	382
Percentage	8.1%	7.1%	8.9%	24.9%	23.8%	27.2%	100

Note: *CS: Computer Science.
**IT: Information Technology.
***CE: Computer Engineering.

Table (2) reveals that the study sample consisted of 31 students in computer maintenance at (8.1%), 27 students in programming technology at (7.1%), 34 in network technology at (8.9%), 95 students in computer science at 24.9%, 91 students in information technology at 23.8% and 104.4 students majoring in computer engineering at 27.2%.

Table 3

Distribution of the study sample according to academic years

Academic Years	First Year	Second Year	Third Year	Fourth Year	Fifth Year	Total
Frequency	113	82	111	41	35	382
Percentage	29.6%	21.5%	29.1%	10.7%	9.2%	100%

Table (3) displays that the study sample consisted of (113) female students in the first year by 29.6%, (82) female students in the second year by 21.5%, (111) female students in the third year by 29.1%, (41) female students in the fourth year by 10.7% and (35) female students in the fifth year by 9.2%.

2.2. Data collection tools

To obtain the data required for addressing the research questions, a questionnaire was employed, selected for its appropriateness to the study objectives, methodological framework, and target population. This choice was informed by a review of prior relevant studies (Alsane et al., 2020; Al-Swat et al., 2020; Ahmad Hamed Alsahfy and Saleh Askol, 2019). In developing the research instrument, key thematic areas were identified, and corresponding items were organized into designated axes according to their original formulations and associated fields. The finalized questionnaire consisted of 38 items aimed at evaluating students' awareness of cybersecurity, encompassing both conceptual understanding and awareness of implementation methods and techniques. The items were categorized into two domains: 11 items related to awareness of cybersecurity concepts and 27 items addressing awareness of cybersecurity methods.

2.2.2. Instrument validity

In its preliminary form, the questionnaire was submitted to a panel of experts specializing in educational technologies, curriculum and instruction, measurement and evaluation, computer science, and information technology. The panel was requested to provide evaluative feedback concerning the clarity, relevance, and domain alignment of each item, as well as to recommend modifications, deletions, or additions deemed appropriate. Based on the evaluators' input, several adjustments were made: items numbered 5, 6, 8, and 10 were deleted; item 3 was revised and reformulated within the "Awareness of Cybersecurity Concepts" domain; items 18, 19, 22, and 27 were also removed. Additionally, two items were combined to form a single item within the "Awareness of Methods for Achieving Cybersecurity" domain. Table 4 presents the final distribution of items in the revised version of the questionnaire.

Table 4

Distribution of the list (paragraphs of the questionnaire) in its final form

No.	Domains	Number of Items
1	Awareness of Cybersecurity Concepts	8
2	Awareness of Methods for Achieving Cybersecurity	20
Overall		28

2.2.3. Construct validity

To verify the validity of the questionnaire statements, an exploratory sample outside the study sample consisting of 30 female students from the Faculty of Computing and Information Technology at Taif University was employed. Table 5 presents these results.

Table 5

Pearson's correlation coefficients between tool statements and the total degree of a domain

Awareness of Cybersecurity Concepts				Awareness of Methods for Achieving Cybersecurity							
No	Correlation	No	Correlation	No	Correlation	No	Correlation	No	Correlation	no	correlation
1	**0.750	6	**0.799	1	**0.650	6	**0.710	11	**0.521	16	**0.654
2	**0.559	7	**0.486	2	**0.657	7	**0.675	12	**0.649	17	**0.632
3	**0.506	8	**0.661	3	**0.594	8	**0.709	13	**0.681	18	**0.726
4	**0.539			4	**0.775	9	**0.578	14	**0.715	19	**0.505
5	**0.758			5	**0.769	10	**0.547	15	**0.725	20	*0.451

* Significance level (0.05) ** significance level (0.01)

Table 5 displays the correlation coefficients between each statement's score and its related domain, which ranged between 0.451 and 0.799. These acceptable values confirm the validity of this tool for collecting study data.

The Pearson correlation coefficient was also calculated between the degree of each axis and the total degree of the resolution. Table 6 shows these results.

Table 6

Pearson's correlation coefficients for axes with the total degree of the resolution

Domains	Items	Correlation
Awareness of Cybersecurity Concepts	8	**0.771
Awareness of Methods for Achieving Cybersecurity	20	**0.964

** significance level (0.01)

Table 6 displays the correlation coefficients between each axis' score and that of the instrument as a whole: (0.771) and (0.964), which are high values that demonstrate it is validity for collecting study data.

2.2.4. Stability of the study tool

The stability of the resolution was verified using Cronbach's alpha stability coefficient, with Table 7 displaying its values for each domain along with their combined stability.

Table 7

Cronbach's alpha coefficient to measure the stability of the resolution

Questioner	Domain	Items	Cronbach's alpha
Cyber security	Awareness of Cybersecurity Concepts	8	0.747
	Awareness of Methods for Achieving Cybersecurity	20	0.915
	Overall	28	0.904

Table 7 displays that Cronbach's alpha coefficient for calculating resolution stability was 0.747 and 0.915, while its total stability was 0.904, showing that this study instrument has excellent reliability, making it suitable for collecting study data.

On a Likert five-point scale, responses were obtained from the study sample according to this gradient: (strongly agree, agree, neither, disagree, and strongly disagree). We then translated this scale quantitatively by assigning each statement a score based on degrees: strongly agree (5) degrees, agree (4) degrees, neither (3) degrees, disagree (2) degrees, and strongly disagree (1) degree.

To determine the response criteria for the Likert quintuple scale, we calculated the lengths of cells on a five-point scale by calculating the range (5-1 = 4) and dividing it by the highest value in the scale to obtain cell length (5/4 = 0.80), then add this value to the lowest value in the scale (one), as shown in Table (8).

Table 8

Likert scale division

Category	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
Scale	1	2	3	4	5
Range	1- less than 1.80	1.80 - less than 2.60	2.60 - less than 3.40	3.40 - less than 4.20	4.20 – 5
Interpretation	V. Low	Low	Moderate	High	V. High

3. RESULTS

3.1. Results Related to the First Question." What level of awareness do students at Taif University's Faculty of Computing and Information Technology have regarding cybersecurity concepts?"

To answer this question, arithmetic averages and standard deviations were calculated from responses. Statements were then organized in descending order according to these averages, as shown in Table 9.

Table 9

Mean and Standard Deviations in the domain of Awareness of Cybersecurity Concepts in a descending order

Rank	No of item	The Items	Mean	SD	Degree
1	5	I am aware of the risks involved with spying on a computer	4.46	0.86	V. High
2	8	I understand that cybersecurity is a digital system, and security measures	4.40	0.91	V. High
3	7	I recognize the need to safeguard computers, smart devices, routers, networks, the cloud, and software	4.29	0.95	V. High
4	6	I am aware of the potential threats posed by a cyber-attack	4.20	1.02	V. High
5	4	Cyber deterrence is the practice of actively countering cyberattacks	4.18	0.95	High
6	1	I am well-versed in the field of cybersecurity	3.86	0.99	High
7	3	Social engineering refers to a set of tricks and techniques used to deceive others into divulging their personal information	3.59	1.26	High
8	2	I know the concept of phishing	3.57	1.16	High
The whole domain			4.07	0.66	High

Table 9 indicates that students from the Faculty of Computing and Information Technology at Taif University had a general average level of awareness regarding cybersecurity concepts of 4.07 with a standard deviation of 0.66, giving them an impressively high score. The arithmetic averages for these axis statements ranged between (3.57) and (4.46).

Table 9 reveals that the phrases " I understand that cybersecurity is a digital system and security measures" and " I am aware of the risks involved with spying on a computer" achieved the highest arithmetic averages of (4.40) and (4.46), respectively, with an impressive score. Conversely, phrases like "I have knowledge of phishing" or "social engineering" had low averages of (3.57) and (3.59), respectively, indicating high scores for them as well.

3.2. Results Related to the Second Question: " What level of awareness do students in the Faculty of Computing and Information Technology at Taif University have regarding methods and tactics for achieving cybersecurity?

To answer this question, arithmetic averages and standard deviations were calculated from responses. Statements were then organized in descending order according to these averages as shown in Table 10.

Table 10

Mean and standard deviations for the domain of awareness of methods for achieving cybersecurity in a descending order

Rank	NO	The Items	Mean	SD	Degree
1	7	I understand the security implications of sharing my password with others.	4.62	0.74	V. High
2	17	Make sure to use secure browsers	4.49	0.84	V. High
3	1	Make sure to choose strong passwords for all the apps and sites I use	4.48	0.87	V. High
4	9	I take care not to open any link that I receive without verifying its identity first.	4.44	0.95	V. High
5	13	Be careful not to reply to text messages similar to those of network operators	4.38	1.01	V. High
6	11	Be careful not to enter untrusted sites	4.35	0.91	V. High
7	15	I use two-factor authentication on social media	4.35	1.04	V. High

8	2	Be careful not to send any important information or data through various technical applications or e-mail	4.26	1.02	V. High
9	5	Keep apps and electronic devices up to date	4.21	1.09	V. High
10	3	Make sure to inform the responsible authorities of any technical breakthroughs that occur to me	4.17	1.11	High
11	8	Be careful not to use Wi-Fi networks in public places	4.11	1.15	High
12	18	I am interested in installing protection programs	4.10	1.11	High
13	12	I choose different passwords for my sites, apps, and accounts	4.07	1.12	High
14	4	Make sure to provide backup copies of data and files to preserve them	4.06	1.12	High
15	20	Make sure you don't allow apps to share your location	3.95	1.23	High
16	10	Read the agreements and contracts requested by websites and applications carefully before registering and participating in them	3.67	1.26	High
17	16	Make sure to change the passwords for apps and websites periodically	3.54	1.32	High
18	6	I encrypt important files when they are sent to others	3.38	1.37	Medium
19	14	I don't open emails from an anonymous source	1.76	1.03	V. Low
20	19	I don't respond to anyone asking me for a code that was sent to my mobile	1.47	0.90	V. Low
The whole domain			3.89	0.47	High

Table 10 reveals that students from the Faculty of Computing and Information Technology at Taif University demonstrated an overall average awareness level of 3.89 with a standard deviation of 0.47, indicating a high level of awareness. The arithmetic means of the individual statements within the axis ranged from 1.47 to 4.62.

Statements numbered 7 and 17 recorded the highest arithmetic means, at 4.62 and 4.49, respectively, reflecting a very high level of awareness. In contrast, statements 10 and 16 yielded the lowest arithmetic means among the high-score range, at 3.67 and 3.54, respectively, yet still indicated a high level of awareness.

Statement number 6 registered an arithmetic mean of 3.38, corresponding to a moderate level of awareness. Statement number 14 recorded an arithmetic mean of 1.76, while statement number 19 obtained a mean of 1.47; both were classified as reflecting a very low level of awareness.

3.3. Results Related to the Third Question: "Are there statistically significant differences (α ≤ 0.05) among the average responses of study sample members regarding awareness of methods for achieving cybersecurity based on variables (degree, specialization, academic year)?"

To determine the degree of awareness among female students at Taif University's Faculty of Computing and Information Technology of methods for cybersecurity, a (T) test was applied to two independent samples to reveal statistical differences in average responses from survey members (as shown in Table 11).

Table 11

The result of the (T) test for two independent samples to determine the differences between the responses of the sample members according to the degree variable

Degree	Levine's Test		N	Mean	SD	D.F	T	Sig.
	F	Sig.						
Diploma	2.11	0.15	92	3.54	0.48	380	-8.87	0.000
Bachelor's			290	4.01	0.41			

Table 11 indicates that the value of (T) reached (-8.87), which is below the significance level (α ≤ 0.05). As the significance level was set at (α ≤ 0.05), there are statistically significant differences between average responses from students at the Faculty of Computing and Information Technology regarding awareness of methods and methods for attaining cybersecurity in favor of those with a bachelor's degree.

3.3.1. Specialization and academic year variables

To assess the degree of awareness among students at Taif University's Faculty of Computing and Information Technology regarding cybersecurity methods according to specialization and academic year, a single variance analysis test was used. As shown in Table 12.

Table 12

ANOVA Results on Differences in Responses by Specialization and Academic Year

Variable	Source of variation	Sum of squares	D.F	Mean squares	F	Sig.
Specialization	Between groups	16.285	5	3.257	17.322	0.000
	Within groups	70.701	376	0.188		
	Total	86.986	381			
Academic Year	Between groups	5.921	4	1.480	6.883	0.000
	Within groups	81.066	377	0.215		
	Total	86.986	381			

Table 12 displays that the test (F) values were (17.322) and (6.883), respectively; their significance level was set at ($\alpha \leq 0.05$), which are statistically significant values when ($\alpha \leq 0.05$) exists between any two averages between study groups; to identify which direction these differences lie, we used Schiffe test as shown in Table 13:

Table 13

The result of the Schiffe post-hoc analysis to determine the direction of differences according to the variables of specialization and academic year

Domain	Specialization (I)	Specialization (J)	Mean Difference	Sig.
Awareness of Methods and Methods of Achieving Cybersecurity	Computer science	Computer Maintenance	0.368	*0.005
	Computer science	Programming Technology	0.659	*0.000
	Computer science	Network Technology and Security	0.457	*0.000
	Information Technology	Computer Maintenance	0.328	*0.022
	Information Technology	Programming Technology	0.619	*0.000
	Information Technology	Network technology and security	0.418	*0.000
	Computer Engineering	Computer Maintenance	0.335	*0.015
	Computer Engineering	programming technology	0.626	*0.000
	Computer Engineering	Network technology and security	0.424	*0.000
	Academic Years (I)	**Academic Years (J)**	**Mean Difference**	**Sig.**
	First year	Second Year	0.246	*0.010
	Third year	Second Year	0.284	*0.002
	Fourth year	Second Year	0.296	*0.026
	Fifth year	Second Year	0.403	*0.001

Note: * ($P \leq 0.05$)

4. DISCUSSION

The findings revealed a high level of cybersecurity awareness among female students at Taif University's Faculty of Computing and Information Technology. This heightened awareness is likely attributable to initiatives by faculty members, such as organizing summer camps and cyber clubs. Mountrouidou et al. (2018) emphasized that educational courses effectively convey the importance of cybersecurity and provide foundational knowledge. Similarly, Alkhodari and Kleibi (2020) highlighted the necessity of promoting cybersecurity awareness through institutional programs that introduce key concepts and strengthen security practices. Supporting this, Aljohani et al. (2021) found that students possess high awareness of cybersecurity threats, in contrast to Tirumala et al. (2016), who reported low awareness levels regarding basic cybersecurity principles.

Further, Taif University’s implementation of Google Developer Student Clubs, focused on cybersecurity topics, likely contributed to increased awareness among female students. The Cybersecurity Department has actively promoted awareness through initiatives such as targeted email campaigns. Alshawabkeh (2019) confirmed that Taif University has enacted effective security measures, improving protection against network breaches. Carlin and Manson (2016) noted that extracurricular activities, including student clubs, internships, camps, competitions, and conferences, significantly develop students’ cybersecurity skills and preparedness for potential cyber threats. Conversely, Moallem (2019) found that many students remain uninformed about data protection mechanisms.

Despite the generally high awareness levels, the study identified lower awareness in specific areas, such as the use of encryption before transmitting files. This aligns with Aljundi and Muhammad (2019), who emphasized the need for applied practice in mastering information security. Alsayegh (2018) also stressed the importance of encrypting electronic transactions to prevent unauthorized access and recommended avoiding emails from unknown sources or unsolicited verification requests. Al-Swat et al. (2020) advocated for educational programs that guide students on safely interacting on social media and recognizing potential cyber threats. Almanea (2022) also emphasized the need to enhance digital competencies to support cybersecurity education. These findings are consistent with Khalid et al. (2018), who reported that, despite general awareness, many students lacked knowledge regarding unsafe websites and protective strategies.

Statistical analysis revealed significant differences in awareness based on students' academic level and specialization. Undergraduate students demonstrated higher awareness and competency, likely due to their more advanced coursework and exposure to cybersecurity principles. Salem et al. (2021) observed that students with a deeper understanding of security exhibited more professional responses to cyber threats. This contrasts with Tibi et al. (2019), who found that computer science students often lacked sufficient awareness of cybercrime and self-protection measures, possibly due to gaps in awareness programming.

Differences were also noted among specializations, with students majoring in Computer Science, Information Technology, and Computer Engineering displaying higher cybersecurity awareness. This may result from their engagement in cybersecurity-related coursework and the integration of digital literacy into their curricula (Frydenberg & Lorenz, 2020; Almanea, 2022). Ashafee et al. (2018) found that information technology students generally showed heightened cybersecurity awareness. However, Garba et al. (2020) concluded that computer science students were more vulnerable to cyber threats, likely due to disparities in academic exposure.

Finally, significant differences were observed across academic years. First-year students exhibited high motivation and enthusiasm toward cybersecurity, striving to demonstrate competence in this area. Kam and Katerattanakul (2014) similarly noted elevated motivation among first-year students, which often correlates with increased awareness. Additionally, third-, fourth-, and fifth-year students showed advanced awareness, likely due to accumulated experience and applied skills. Quisumbing (2019) supported this finding, indicating that awareness and comprehension of information security improve with academic progression. However, these results contrast with Mai and Tick (2021), who found generally low cybersecurity awareness among students regardless of academic year, perhaps due to differences in academic focus or specialization.

5. CONCLUSION

The study recommends the organization of comprehensive cybersecurity training courses, including content addressing the risks associated with data sharing. Additionally, the establishment of student organizations such as the Cybersecurity Club and the Technology and Programming Club is advised, with a focus on applied topics within the Faculty of Computing and Information Technology. Emphasis should also be placed on enhancing student awareness of cyber-attack threats through educational initiatives led by cybersecurity experts.

The findings of the current study contribute significantly to understanding the level of cybersecurity awareness among students. Nevertheless, several limitations must be acknowledged. The participant pool was restricted to female students at Taif University, and the limited sample size, combined with reliance on a single data collection instrument, restricts the generalizability of the findings across institutions and academic disciplines.

In light of the results and proposed recommendations, further research within Arab contexts is warranted to explore various dimensions of cybersecurity. Suggested areas of investigation include studies on cognitive competence related to cybersecurity and resilience against cyberattacks among student populations, as well as experimental research to evaluate the effectiveness of Capture the Flag platforms in enhancing cybersecurity capabilities. Future research should involve a larger and more diverse sample, employ multiple

and methodologically robust instruments informed by cybersecurity experts, and encompass various academic disciplines and demographic groups.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The author would like to thank the Deanship of Scientific Research at Taif University and Professor Dr. Mohammed Khair Alsalamat for supporting this work.

Conflict of Interest: The authors declare no conflict of interest.

Ethical Approval: The study adheres to the ethical guidelines for conducting research.

Funding: This research received no external funding.

REFERENCES

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379. https://www.academia.edu/download/70021757/8222.pdf

Adeshola, I., & Oluwajana, D. I. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*, 1-23. https://link.springer.com/article/10.1007/s40692-024-00346-7

Ahmad Hamed Alsahfy, M., & Saleh Askol, S. (2019). The Level of Computer Teachers' Awareness of Cybersecurity in Secondary Schools in Jeddah. *Journal of Scientific Research in Education*, *20*(10), 493-534. https://jsre.journals.ekb.eg/article_56490.html?lang=en

Albishi, M. A. (2021). Cybersecurity in Saudi universities and its impact on enhancing digital trust from the point of view of faculty members: a study on the University of Bisha. *Islamic University Journal of Educational and Psychological Studies, 29*(6), 353-372.

Aldhawifri, M. S. (2021). The reality of cybersecurity and increasing its effectiveness in public education schools in the Medina region from the point of view of school leadership. *International Journal of Educational and Psychological Studies, 10*(3), 635-655.

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia University students. *International Journal of Advanced Computer Science and Applications*, *12*(3), 276-281. https://www.academia.edu/download/86150147/Paper_34-Cybersecurity_Awareness_Level.pdf

AlJundi, A. A. I., Mohammed, N. T. H (2019). The role of applied practice of cybersecurity in developing the skills and accuracy of the practical application of information security among university students. *Journal of World of Education, 3*(67), 14-84.

Alkhathami, M. D. (2020). The level of awareness of information security issues among secondary school students in public schools in Riyadh. *Journal of Humanities and Social Sciences, 47*, 355-400.

Alkhodari, J. Salami, H. & Kleibi, N. (2020). Cybersecurity and Artificial Intelligence in Saudi Universities. *Journal of University Performance Development, 12*(1), 217-233.

Almanea, A. A. I. (2022). Requirements for achieving cybersecurity in Saudi universities in light of 2030. *Scientific Journal of the Faculty of Education, 38*(1), 155-194.

Almuntashari, F. Y. (2020). The degree of awareness of middle school teachers about cybersecurity in public schools in Jeddah from the teachers' point of view. *Arab Journal of Specific Education, 4*(14), 95-140.

Alqahtani, M. A. (2022). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Computational Intelligence and Neuroscience*, *2022*(1), 6775980. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/6775980

Alqahtani, M., & Kavakli-Thorne, M. (2023). A systematic review of current cybersecurity training methods. *Computers & Security, 127*, 102648. https://doi.org/10.1016/j.cose.2023.102648

Alqahtani, N. N. (2019). The availability of cybersecurity awareness among male and female students of Saudi universities from a social perspective: a field study. *Sharjah Sociologist Society, 36(*144), 85-120.

Alsane, N., Al-Swat, H., Abu Eisheh, Z., Suleiman, E. &Asran, A. (2020). Teachers' awareness of cybersecurity and methods of protecting students from Internet risks and enhancing their national values and identity. *Scientific Journal of the Faculty of Education, Assiut University, 36*(6), 41-90.

Alsayegh, W. H. (2018). Family members' awareness of the concept of cybersecurity and it is relationship to their security precautions from cybercrime, Saudi Arabia. *Arab Journal of Social Sciences, 14*(3), 18-70.

Alshawabkeh, A. A. (2019). The role of information security measures in reducing information security risks at Taif University. *Journal of Studies and Research, 11*(4), 164-187.

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., ... & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia. *Information*, *12*(5), 208. https://www.mdpi.com/2078-2489/12/5/208

Al-Swat, H. H., Alsana, N. O. A., Abu-Eisheh, Z. J., Soliman, E. M., & Assran, A. S. E. A. (2020). The Relationship between Cyber-Security Awareness and the National, Moral, and Religious Values of Primary and Intermediate School Students in Taif. *Journal of Scientific Research in Education*, *21*(4), 278-306. https://jsre.journals.ekb.eg/article_92657_en.html?lang=en

Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). The four most famous cyber attacks for financial gains. *Int. J. Eng. Adv. Technol*, *9*, 2131-2139. https://www.researchgate.net/profile/Jehad-Al-Amri/publication/341113382_Four_Most_Famous_Cyber_Attacks_for_Financial/links/5eaee60ba6fdcc7050a6c9f1/Four-Most-Famous-Cyber-Attacks-for-Financial.pdf

Amin, M., Alam, N., Dhahir, D. F., & Hadiyat, Y. D. (2021). Security and privacy awareness of smartphone users in Indonesia. In *Journal of Physics: Conference Series, 1882*(1), 012134. https://iopscience.iop.org/article/10.1088/1742-6596/1882/1/012134/meta

Ashafee, T. L., Moh, S., Zakaria, N. H., Mohamad Tahir, H., Katuk, N., & Omar, M. N. (2018). Security behaviors on social network sites used for academic purposes: a comparison of security preparedness and awareness among IT and non-IT postgraduate students. *The Journal of Social Sciences Research*, (SPI6), 839-846. https://repo.uum.edu.my/id/eprint/26453/

Bock, K., Hughey, G., & Levin, D. (2018). King of the hill: A novel cybersecurity competition for teaching penetration testing. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. https://www.usenix.org/conference/ase18/presentation/bock

Carlin, A., & Manson, D. (2016). POLYTECHNIC EDUCATION FOR THE CYBERSECURITY WORKFORCE. *Strategic Finance*, *98*(1). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=1524833X&asa=N&AN=116574154&h=db9mlwP8260M9i9wQ2UNnAS7yIKMiwqZ78joX6Vf3XwW444tK8B%2BqnEr4bUIcH8WbVAINlmMMwrqfBmns%2BR8uQ%3D%3D&crl=c

Christen, M., Gordijn, B., &loi, M. (2020). *The ethics of cybersecurity*. Springer publishing.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://www.sciencedirect.com/science/article/pii/S0166361522000094

Dam, D. L. (2020). Relationship Between Demographic Variables and Awareness on Cybersecurity Threats: An Empirical Analysis. *The Orissa Journal of Commerce*, *41*, 112-122. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789806

Faraj, A. O. K., (2022). Reasons to promote a culture of cybersecurity in light of digital transformation Prince Sattam bin Abdulaziz University as a model. *Educational Journal of the Faculty of Education Sohag, 1*(94), 509-537.

Frydenberg, M., & Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, *18*(4), 33-45. https://eric.ed.gov/?id=EJ1258201

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *Int. J. Emerg. Technol*, *11*(5), 41-49. https://www.academia.edu/download/64160387/A%20Study%20on%20Cybersecurity%20Awareness.pdf

Gelernter, N., Kalma, S., Magnezi, B., & Porcilan, H. (2017). The password reset MitM attack. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 251-267). https://ieeexplore.ieee.org/abstract/document/7958581/

Goran, I. (2017). Cyber security risks in public high schools. https://academicworks.cuny.edu/jj_etds/5/

Graham, J., Olson, R., & Howard, R. (Eds.). (2016). *Cyber security essentials*. CRC Press. https://books.google.com/books?hl=en&lr=&id=hu4bJo5v3dsC&oi=fnd&pg=PP1&dq=Graham,+J.,+Howard,+R.,+Olson,+R.+(2011).+Cyber+Security+essentlals.+CRC+Press.%E2%80%8F%E2%80%8F&ots=VqSiE4_LhI&sig=POg3SYLPO9mMhZ1M8hWMI2r27aA

Howell, C., Maimon, D., Muniz, C., Kamar, E., & Berenblum, T. (2024). Engaging in cyber hygiene: the role of thoughtful decision-making and informational interventions. *Frontiers in Psychology*, *15*, 1372681. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2024.1372681/full

Jaballah, A. M. A. (2022). Means of protecting cybersecurity - an original jurisprudential study compared to contemporary systems. *Journal of the Faculty of Sharia and Law, Assiut, 34*(3), 2231-2296.

Johnson, M. (2022). Cybersecurity education, awareness raising, and training initiatives: A review of effectiveness. *Computers & Security, 112*, 102522. https://doi.org/10.1016/j.cose.2022.102522

Kam, H. J., & Katerattanakul, P. (2014). Out-Of-Class Learning: A Pedagogical Approach of Promoting Information Security Education. https://www.researchgate.net/profile/Hwee-Joo-Kam/publication/263278022_Out-Of-Class_Learning_A_Pedagogical_Approach_of_Promoting_Information_Security_Education/links/0f31753a6b4060c263000000/Out-Of-Class-Learning-A-Pedagogical-Approach-of-Promoting-Information-Security-Education.pdf

Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity policy and strategy management in fintech. *Understanding cybersecurity management in fintech: challenges, strategies, and trends*, 153-166. https://link.springer.com/chapter/10.1007/978-3-030-79915-1_8

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(4.21), 11-14. https://www.academia.edu/download/57921354/IJET-21607_1.pdf

Khan, W. N., Lee, J. K., & Liu, S. (2025). Is Cybersecurity a Social Responsibility?. *Information Systems Frontiers*, 1-25. https://link.springer.com/article/10.1007/s10796-024-10565-z

Kolenko, M. M. (2019). *Cyber defender cultural patterns and operational behavior* (Doctoral dissertation, Capitol Technology University). https://search.proquest.com/openview/2a6073789b23e011abce4715a9ca224d/1?pq-origsite=gscholar&cbl=18750&diss=y

Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, *23*(1), 16-24. https://sciendo.com/pdf/10.2478/raft-2018-0002

Kritzinger, E. (2017). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review*, *14*(1), 22-41. https://www.tandfonline.com/doi/abs/10.1080/18146627.2016.1224561

Kucek, S., & Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (ctf) environments. *Journal of Network and Computer Applications*, *151*, 102470. https://www.sciencedirect.com/science/article/pii/S1084804519303303

Leune, K., & Petrilli Jr, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th annual conference on information technology education* (pp. 47-52). https://dl.acm.org/doi/abs/10.1145/3125659.3125686

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, *18*(8), 67-89. https://www.researchgate.net/profile/Andrea-Tick-2/publication/354864771_Cyber_Security_Awareness_and_Behavior_of_Youth_in_Smartphone_Usage_A_Comparative_Study_between_University_Students_in_Hungary_and_Vietnam/links/615466fe2b348727820025e7/Cyber-Security-Awareness-and-Behavior-of-Youth-in-Smartphone-Usage-A-Comparative-Study-between-University-Students-in-Hungary-and-Vietnam.pdf

Ministry of Education. (2020). Ministry of Education and National Cybersecurity Authority. https://www.moe.gov.sa/ar/mediacenter/MOEnews/Pages/am1442-876.aspx

Moallem, A. (2019). *Cybersecurity awareness among students and faculty*. CRC Press. https://www.taylorfrancis.com/books/mono/10.1201/9780429031908/cybersecurity-awareness-among-students-faculty-abbas-moallem

Mohammed, H. H. M. (2020). A proposed program based on the geography of cyber wars to develop awareness of their dangers and promote the values of digital citizenship for student teachers in the College of Education. *Journal of the Faculty of Education in Educational Sciences, 44*(3), 81-150.

Mountrouidou, X., Li, X., & Burke, Q. (2018). Cybersecurity in liberal arts general education curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp. 182-187). https://dl.acm.org/doi/abs/10.1145/3197091.3197110

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity*, *800299*. https://ibimapublishing.com/uploads/articles/JIACS/2017/800299/800299.pdf

Nasser Mohamed Alshahrani, B., & Flemban, F. Y. (2020). The impact of a training program based on designing electronic games using Game Maker to enhance cyber security concepts for middle-school students. *Journal of Scientific Research in Education*, *21*(9), 614-651. https://jsre.journals.ekb.eg/article_128494.html?lang=en

National Cybersecurity Authority. (2018). Basic Cybersecurity Controls, https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., Blanc, G., & Kadobayashi, Y. (2019). An empirical approach to phishing countermeasures through smart glasses and validation agents. *Ieee Access*, *7*, 130758-130771. https://ieeexplore.ieee.org/abstract/document/8830416/

Nyinkeu, N. D., Anye, D., Kwedeu, L., & Buttler, W. (2018). Cyber Education outside the Cyberspace: The case of the Catholic University Institute of Buea. *International journal of technology in teaching and learning*, *14*(2), 90-101. https://eric.ed.gov/?id=EJ1211986

Olsen, R. V., & Tokerud, S. (2020). *Teachers' awareness, knowledge, and practice of information security in school* (Master's thesis, University of Agder).

Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being Responsible in Cybersecurity: A Multi-Layered Perspective. *Information Systems Frontiers*, 1-19. https://link.springer.com/article/10.1007/s10796-025-10588-0

Patel, R. (2021). A Research of the awareness level among Technical and Non-technical students of cyber security in Parul University. *International Research Journal of Management Sociology & Humanity, 12*(2), 116-119.

Qiu, S., Xu, G., Ahmad, H., Xu, G., Qiu, X., & Xu, H. (2019). An improved lightweight two-factor authentication and key agreement protocol with dynamic identity based on elliptic curve cryptography. *KSII Transactions on Internet and Information Systems (TIIS)*, *13*(2), 978-1002. https://koreascience.kr/article/JAKO201914260133365.page

Quisumbing, L. A. (2019). Preemptive Evaluation through information security awareness: Perception of information technology students in a Philippine State University. *International Journal of Applied Engineering Research*, *14*(4), 900-907. https://www.academia.edu/download/87478188/ijaerv14n4_09.pdf

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*, *12*(3), 1598. https://www.mdpi.com/2076-3417/12/3/1598

Rege, M., & Mbah, R. B. K. (2018). Machine Learning for Cyber Defense and Attack (paper presentation). The Seventh International Conference on Data Analytics, Athens, Greece.

Sabbagh, M. H. (2021). *Digital Security Guide*. Hsoub Academy.

Sabq newspaper (2021), the launch of the "@Hack" conference in Riyadh with the participation of cybersecurity geniuses in the world, published on 28/11/2021.

Salem, Y., Moreb, M., & Rabayah, K. S. (2021). Evaluation of information security awareness among Palestinian learners. In *2021 International Conference on Information Technology (ICIT)* (pp. 21-26). IEEE.