PISSN : 2571-9904 - EISSN : 2602-7763

The Gap Between Awareness and Practice in Cybersecurity Among Specialized Students: A Field Study on a Sample of Students at the Higher School of Cybersecurity in Algeria

Debihi Ouafa[1*], Rahali Miloud[2]

[1] university of blida2 lounici ali,Blida (Algeria) , o.debihi.etu@univ-blida2.dz
[2] university of blida2 lounici ali,Blida(Algeria),m.rahali@univ-blida2.dz

Received: 25 / 05 / 2026 **Accepted**: 25 / 07 / 2026 **Published**: 31 / 07 / 2026

Abstract:
This study examines the cybersecurity awareness level and actual practices among students at the Higher School of Cybersecurity in Algeria. Utilizing a descriptive-analytical approach, the researcher administered a questionnaire to a purposive sample of 100 students. The findings revealed that while students' awareness was high and general practices were good, behaviors were limited to basic measures like strong passwords, showing weakness in institutional practices like incident reporting. Additionally, students faced key challenges including high costs of security tools, lack of training, and difficulties with two-factor authentication. Statistical analysis showed awareness differences favoring third-year students and practice differences favoring those with advanced technical expertise. Ultimately, a strong correlation confirmed that enhancing knowledge directly improves students' security behaviors.

Keywords: *Cybercrime; Cybersecurity;Digital Awareness; Preventive Practices; Students of the Higher School of Cybersecurity.*

Debihi Ouafa

I. INTRODUCTION

With the rapid development of information technologies and the widespread adoption of the internet, reliance on digital platforms has become an essential part of university students' lives, particularly at the Higher School of Cybersecurity. Students use these platforms to conduct their various academic activities, including e-learning, accessing databases, managing research projects, following courses, and communicating with peers and supervisors.

Despite the significant opportunities these tools offer for learning and collaboration, their increasing reliance exposes students to real cybersecurity risks that could compromise the integrity of their data and information security, especially if preventative practices are weak or appropriate security measures are absent. These risks include various threats such as malware, hacking, leaks of sensitive information, and online fraud.

This reality underscores the urgent need to cultivate a cybersecurity culture and translate theoretical awareness into practical application among students in specialized fields to ensure the protection of both personal and academic data. This study aims to highlight the gap between students' level of cybersecurity awareness and their practical behaviors, enabling an understanding of the shortcomings and the development of recommendations to enhance digital security within a specialized academic environment.

In this context, cybersecurity has emerged as one of the most pressing issues for both educational and research institutions. Cybersecurity refers to "the measures taken to protect computers and networks from unauthorized access, ensuring the integrity of information. This includes technical interventions that protect data, identity information, and devices from breaches or damage" (Richardson et al., 2020,p.15). However, cybersecurity is not limited to the technical aspect alone; it also encompasses the level of awareness and behaviors adopted by users when interacting with digital technologies. Numerous studies have confirmed that a lack of security awareness is one of the most prominent reasons for the success of cyberattacks. This places a heightened responsibility on educational institutions to promote a culture of digital security among their students through effective awareness and training programs. For example, the Al-Awda study (2025) indicated that a lack of awareness and poor practical application of protection measures increase the vulnerability of individuals and institutions to breaches and data theft, calling for the strengthening of legislation, infrastructure, and awareness as part of the national security system. Hence the importance of this research, which seeks to analyze the level of awareness among graduate students in the College of Education regarding the concept of cybersecurity and their related practices, and to uncover the challenges and obstacles they face in this field. This contributes to developing practical recommendations to promote a culture of digital security in the academic environment, which helps ensure the protection of sensitive data and information and maintain the integrity of educational systems and networks.

Research Problem : To what extent does the level of cybersecurity awareness among students of the Higher School of Cybersecurity in Algiers reflect on their preventive digital practices and behaviors?

-1Research Questions: The main question is differentiated into the following sub-questions

-What is the level of awareness among students of the Higher School of Cyber Security in Algiers regarding the concept and importance of cybersecurity?

- What are the prominent cybersecurity measures implemented by students of the Higher School of Cyber Security in Algiers when utilizing digital technologies?

-What challenges and difficulties do students of the Higher School of Cyber Security in Algiers face in complying with cybersecurity measures?

- What proposals could contribute to promoting a cybersecurity culture among students of the Higher School of Cyber Security in Algiers?

2.Objectives of the study:

-To identify the level of awareness among students at the Higher School of Cybersecurity at the University of Algiers regarding the concept of cybersecurity and its importance in the academic environment.

-To analyze the actual practices of students at the Higher School of Cybersecurity when using digital technologies in light of cybersecurity procedures.

- To identify the most prominent challenges and difficulties that students face in adhering to cybersecurity procedures.

- To provide practical recommendations that contribute to enhancing cybersecurity culture among students at the Higher School of Cybersecurity at the University of Algiers.

3.Significance of the study:

This research stems from several theoretical and applied aspects, which can be explained as follows:

3.1 Theoretical Significance:

-This research contributes to enriching the educational literature related to cybersecurity in higher education by focusing on graduate students, a group often underrepresented in previous studies compared to undergraduate students or academic staff.

-It contributes to building a knowledge framework that helps researchers understand the relationship between cybersecurity awareness and actual practices in the academic environment. It may also pave the way for future studies addressing other aspects.

3.2 Applied Significance:

-The research provides real-world data that graduate school administrations can utilize in developing policies and training programs to enhance cybersecurity culture among graduate students.

-It helps identify behavioral and technical vulnerabilities that may expose students to security risks, enabling educational institutions to develop effective preventative measures.

- It contributes to raising the level of digital security in the higher education environment, which positively impacts the quality of scientific research and the protection of intellectual property.

- This can form the basis for designing awareness campaigns or courses that integrate cybersecurity concepts into graduate programs.

II. Theoretical Framework and previous studies:

1. Theoretical Framework&Concepts

1.1 cybersecurity: The term cybersecurity emerged in the early 1990s when researchers and specialists in computer science and information technology began searching for solutions and procedures to mitigate the risks and threats facing computers, networks, and their systems. The term originates from the concept of "cybernetics," derived from the word "cyber," which is related to the Greek term "cybernetics," meaning "direction and control." Norbert Witter used the ancient Greek word "kybernetes," meaning "steerer," referring to the person who steers a ship. The description is the principle of managing and directing systems and machines, which was later translated into English as "Beer, Cybernetics".

The scientific literature has addressed the concept of cybersecurity with multiple definitions. The European Commission defined it as "the activities necessary to protect networks, information systems, their users, and other persons affected by cyber threats." It is also defined as "the measures taken to protect" (European Commission, 2020, p. 15) by safeguarding data, computers, and networks from unauthorized access, thus ensuring the integrity and security of information. This includes technical interventions that protect data, identity information, and

devices from breaches or damage (Richardson et al., 2020, p. 15). Al-Saadat and Al-Tamimi defined it as awareness of illegal practices that aim to breach, disrupt, modify, or exploit data and information without authorization, with the goal of preventing them (Al-Saadat and Al-Tamimi ,2022,p. 249). While Abu Hussein views cybersecurity as a field concerned with the procedures and standards of protection that must be adhered to in order to confront threats and mitigate their effects in the worst-case scenario (Abu Hussein Hanin , 2021 , p. 18), Hantouli and Al-Zuboun broaden the concept to encompass a set of technical means and methods, electronic processes and procedures, organizational and administrative measures, mechanisms, programs, and digital applications that provide protection and safety for information systems, data, networks, platforms, computers, and smart devices from threats, dangers, and cybercrimes, securing them from unauthorized access, misuse, and threats to their confidentiality and privacy in the vast cyberspace (Hantouli , Al-Zuboun,2025,p. 18). Haswa and Al-Qudah add that cybersecurity includes procedures and technologies aimed at protecting data and systems from any illegitimate interference that could lead to device disruption or information manipulation (Haswa ,Al-Qudah,2023,p. 64). From the above, we find that cybersecurity is a set of technical, organizational, and administrative procedures and measures aimed at protecting information systems, networks, digital devices, and data stored or exchanged via cyberspace from any unauthorized access. Or unlawful exploitation, by ensuring the confidentiality, integrity, timeliness, and availability of information, and by mitigating cyber risks and threats that could disrupt services or harm individual and institutional interests.

1. 2 Cybercrimes: The misuse of information and communication technologies by offenders is referred to as internet crimes, computer misuse, computer-related crime, high-tech crime, and cybercrime. The Association of Chief Police Officers defines it as "the use of computer or internet networks and technology to commit or facilitate the commission of a crime." The Australian Institute of Criminology considers it "a general term for crimes committed using electronic data storage or a communications device." (Bara, 2017, p. 259).

1. 3 Cyber Awareness: Personal cyber awareness refers to an individual's perception and understanding of cyber risks and threats within the digital environment, and the extent to which this awareness influences their knowledge, attitudes, and behaviors toward adopting safe and responsible digital practices. Cyber awareness is a dynamic concept that interacts with knowledge. Cybersecurity and risk perception contribute to shaping how individuals recognize, interpret, and respond to digital threats. (McGregor et al., 2025, p. 7).

1.4 Preventive Practices: Securing cyberspace has become a pressing necessity for both individuals and organizations, given the increasing number of cyber threats and the complexity of modern networks. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recommends following a set of best practices to mitigate risks. These include: using strong and unique passwords for each account; regularly updating software and operating systems to patch vulnerabilities; enabling multi-factor authentication (MFA) to restrict unauthorized access; and performing regular data backups to ensure recovery when needed. The agency also emphasizes the importance of network partitioning and access control to improve the protection of sensitive systems and data. These practices are essential for promoting "cyber hygiene" and significantly reducing cyber risks. (CISA 2025).

1.5 Students of the Higher School of Cybersecurity: Operationally defined as: students enrolled at an Algerian university specializing in the Higher School of Cybersecurity. They will pursue their studies during the 2025-2026 academic year.

2.Previous Studies:

-A study by Ben Berghout (2023), titled "Cybersecurity and the Protection of Digital Data Privacy in Algeria in the Era of Digital Transformation and Artificial Intelligence," aimed to reveal the reality of cybersecurity in Algeria, focusing on the protection of digital data amidst rapid digital transformation. The study adopted a descriptive approach by analyzing official statements and documents related to security policies.

The study concluded that Algeria faces a range of increasing cyber threats, especially with the expanding use of technology and artificial intelligence, which makes digital data vulnerable to hacking and exploitation. It also highlighted challenges related to the implementation of security policies and a lack of digital awareness, contrasted with government efforts to develop protection mechanisms and strengthen digital infrastructure.

-A study by Qashir Saleh (2025), titled "Digital Sovereignty and Cybersecurity: Legal and Strategic Dimensions in Algeria," aimed to analyze the relationship between cybersecurity and digital sovereignty in the Algerian context, considering them as pillars of national security in the digital age. The study, based on legal and strategic analysis, concluded that achieving digital sovereignty in Algeria depends on the state's ability to secure its digital infrastructure and protect its data from external dependence. The study also emphasized the importance of developing national legislation, investing in local technology, and developing human capital, particularly in the cybersecurity field.

- A study by Vigit (2025) titled "The Role of Mindfulness as an Influencing Factor in Cybersecurity Behaviors Among Undergraduate Students" aimed to investigate the predictive effect of mindfulness on cybersecurity behaviors among undergraduate students. The study, conducted using a descriptive methodology, included 179 undergraduate students enrolled at a public university. Data were collected through an online questionnaire using the "Personal Cybersecurity Provision Scale" and the "Mindfulness Scale." The results showed no statistically significant differences in cybersecurity behaviors between male and female students. Differences were observed only between departments in cybersecurity behaviors, specifically between the Primary Mathematics Teacher Training Department and the Turkish Language Teacher Training Department, with students in the former exhibiting better behaviors. No differences in cybersecurity behaviors were observed between different academic years. A moderate positive correlation was found between mindfulness and cybersecurity behaviors, with mindfulness explaining 9.4% of the variance in cybersecurity behaviors. Finally, analysis of adjusting factors revealed that gender, department, and academic year did not significantly influence this effect.

- A study by Boochet et al. (2024), titled "Cybersecurity Awareness and Cybersecurity Behaviors Among High School Students in Davao City: A Mediating Role for Perceived Behavioral Control," aimed to determine the mediating role of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behaviors among high school students in Davao City, Philippines. Based on planned behavior theory and using a quantitative approach, data were collected through a questionnaire distributed to 100 male and female students at a private high school in Davao City. Validated measures were used to assess cybersecurity awareness, perceived behavioral control, and cybersecurity behaviors, while strictly adhering to ethical considerations and data confidentiality. The study revealed that high school students generally exhibit a high level of cybersecurity awareness, perceived behavioral control, and responsible cybersecurity behaviors. However, there is still room for improvement, particularly in promoting responsible behaviors in this area. Furthermore, the study revealed a moderate and statistically significant positive correlation between cybersecurity awareness and responsible behaviors. In this area, the findings indicate that increased awareness leads to more responsible cybersecurity behavior. Furthermore, a statistically significant relationship exists between perceived behavioral control and responsible behavior in this area, suggesting that students who feel more in control of their cybersecurity actions tend to exhibit better behaviors. The results also highlight the mediating role of perceived behavioral control in the relationship between cybersecurity awareness and responsible behavior. This suggests that perceived behavioral control plays a crucial role in influencing how cybersecurity awareness translates into actual behaviors among secondary school students.

3-Commentary on Previous Studies

The presented previous studies reveal a growing interest in cybersecurity from multiple perspectives, combining strategic, legal, and behavioral dimensions. This reflects the complex nature of this field in light of rapid digital transformation.

On the one hand, macro-level studies, such as those by Ben Berghout (2023) and Qashir Saleh (2025), focused on analyzing the reality of cybersecurity in Algeria from an institutional and strategic perspective. They highlighted the challenges related to securing digital infrastructure, weak cybersecurity awareness, and the issues of digital sovereignty and technological dependency. These studies are commendable for linking cybersecurity to national security issues and digital development. However, they remained within a theoretical analytical framework and did not delve into the fieldwork of individual behavior, particularly among students.

In contrast, micro-level studies, such as those by Vigit (2025) and Boochet et al. (2024), focused on analyzing individual behaviors related to cybersecurity, emphasizing the role of awareness, psychological factors, and behavioral explanatory models (such as planned behavior theory). These studies have demonstrated a positive correlation between cyber awareness and safe behaviors, highlighting mediating variables such as perceived behavioral control, which enriches the behavioral understanding of cybersecurity. However, these studies were conducted in foreign contexts, limiting the generalizability of their findings to the Algerian environment without field testing.

At the comparative level, a complementary approach is observed between the two approaches; the former addresses the macro level (policies and legislation), while the latter focuses on the individual level (behavior and awareness). Nevertheless, this complementarity remains underutilized in studies that combine both dimensions simultaneously.

Consequently, a clear research gap exists: the absence of field studies in the Algerian context that link the level of cyber awareness with students' actual practices, taking into account institutional and strategic dimensions. This justifies the importance of the current study, which seeks to explore this relationship empirically and contribute to bridging this knowledge gap.

III.Methods and Materials :

The researcher adopted the descriptive survey method as it is the most suitable for studying the level of awareness among students at the Higher School of Cybersecurity. This method allows for the collection of quantitative data from a large sample and its statistical analysis to reach accurate conclusions. Using this method, the researcher developed a questionnaire to assess the current state of cybersecurity at the school.

This questionnaire was then administered to the research sample, and the data was collected, described, and analyzed using appropriate statistical methods. The results were then discussed and reviewed in light of previous studies and field observations.

1. Research Population and Sample

The original population: The original research population consisted of 100 students (male and female) at the Higher School of Cybersecurity, University of Algiers, 2025-2026. The research sample was selected using purposive sampling. The sample was chosen intentionally based on its suitability to the research topic and its possession of specific characteristics relevant to the study. The sample size consisted of (100) male and female students, selected according to specific criteria to ensure the achievement of the study objectives and the acquisition of scientifically significant data.

2. the research instrument:

Achieving the research objectives and verifying its hypotheses required the use of a questionnaire developed by the researcher. The questionnaire was initially prepared after reviewing the theoretical literature, previous studies, and some research tools related to cybersecurity.

3. The limitations of the study:

- Human Limitations: Students of the Higher School of Cybersecurity.
- Subject Limitations: Awareness and preventive practices in the field of cybersecurity

-Time Limitations: This study was conducted during the period from October to November, during which the research instrument was developed, field data was collected, and statistically processed.

IV.Result And Discussion

1. Presentation of statistical results:

Table (1) : Presenting the Results

Variable	N	Arithmetic Mean	Standard Deviation	Minimum	Maximum
Daily Usage	100	2.15	0.48	1	3
Number of Accounts	100	1.97	0.73	1	3

The source : Descriptive Statistics

The results in Table (1) show that the average daily usage was (2.15) with a standard deviation of (0.48), with values ranging between a minimum of (1) and a maximum of (3). The average number of digital accounts was (1.97) with a standard deviation of (0.73), with the same minimum and maximum limits.

Table (2) : Sample Distribution by Gender

Gender	Frequency	Percentage
Male	58	58.0%
Female	42	42.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (2) show the distribution of the sample members by gender, where males outnumbered females in the studied sample.

Table (3) : Reporting Cyber Threats

Reporting	Frequency	Percentage
No	24	24.0%
Yes	76	76.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (3) show that the majority of the sample report cyber threats, while a minority do not.

Table (4): Legal Awareness of Cybercrimes

Legal Awareness	Frequency	Percentage
No	23	23.0%
Yes	77	77.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (4) show that the majority of respondents possess legal awareness of cybercrimes, while a smaller percentage lack this awareness.

Table (5): Developing Protection Methods

Developing Protection	Frequency	Percentage
No	21	21.0%
Yes	79	79.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (5) show that most members of the sample have developed digital protection methods, while a limited percentage have not.

Table (6): Adopting New Protection Methods

New Protection Methods	Frequency	Percentage
No	59	59.0%
Yes	41	41.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (6) show that less than half of the sample adopt new protection methods, while the majority do not.

Table (7): Cybersecurity Training

Training	Frequency	Percentage
No	100	100.0%
Yes	0	0.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (7) show a lack of cybersecurity training among all members of the sample.

Table (8): Regular System Updates

Update	Frequency	Percentage
No	82	82.0%
Yes	18	18.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (8) show that the majority of the sample do not update their systems regularly, while a limited percentage do.

Table (9): Respect for Confidentiality

Confidentiality	Frequency	Percentage
No	39	39.0%
Yes	61	61.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (9) show that more than half of the sample adheres to confidentiality, while a smaller percentage does not.

Table (10): Use of Encryption

Encryption	Frequency	Percentage
No	38	38.0%
Yes	62	62.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (10) show that the majority of the sample use encryption technologies, while a minority do not.

Table (11): Malware Detection

Malware Detection	Frequency	Percentage
No	33	33.0%
Yes	67	67.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (11) show that the majority of respondents use methods to detect malware, while a smaller percentage do not.

Table (12): Facebook Use

Facebook Use	Frequency	Percentage
No	69	69.0%
Yes	31	31.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (12) show that less than half of the sample uses the Facebook platform.

Table (13): Twitter (X) Use

Twitter Use	Frequency	Percentage
No	88	88.0%
Yes	12	12.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (13) show the limited use of the Twitter (X) platform among the sample.

Table (14): YouTube Use

YouTube Use	Frequency	Percentage
No	73	73.0%
Yes	27	27.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (14) show that the use of the YouTube platform is relatively limited among the respondents.

Table (15): Instagram Use

Instagram Use	Frequency	Percentage
No	65	65.0%
Yes	35	35.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (15) show that Instagram is the most used platform relatively compared to the other platforms.

Table (16): Other Preventive Measures

Other Preventive Measures	Frequency	Percentage
No	100	100.0%
Yes	0	0.0%
Total	100	100%

The source : prepared by the researchers

The results in Table (16) show that the sample did not adopt any other digital preventive measures besides those mentioned.

Table (17): Summary of Cybersecurity Practices Among the Sample

Variable	No	Yes
Legal Awareness	24%	76%
Reporting Threats	23%	77%
Developing Protection Measures	21%	79%
Adopting New Measures	59%	41%
Regular Updates	82%	18%
Respecting Confidentiality	39%	61%
Using Encryption	38%	62%
Detecting Malware	33%	67%

The source : prepared by the researchers

Table (17) presents a synthesis of the level of cybersecurity practices among the sample.

2.Discussion of Results:

The study results show that the sample group possesses a considerable level of legal awareness regarding the risks of cybercrime, which is reflected in their positive willingness to report digital threats. This can be explained by the link between legal knowledge and preventative behavior, as understanding the legal dimensions contributes to promoting responsible handling of cyber risks.

However, this theoretical awareness is not fully reflected in daily practice. The results reveal weaknesses in some basic preventative behaviors, such as regularly updating systems and limited adoption of new protection methods. This discrepancy highlights a clear gap between theoretical knowledge and practical application.

These results are particularly significant given that the sample consists of students from the Higher School of Cybersecurity, a group expected to possess specialized technical knowledge. However, the results indicate that academic training, despite its specialized nature, does not necessarily guarantee the establishment of sustainable daily preventative practices outside the educational setting.

Furthermore, the lack of formal practical training reveals that students rely on individual efforts and personal experience rather than structured institutional training, which is reflected in the limited diversification of adopted preventative measures. Regarding the development of protection measures, it is observed that this development remains limited to basic

functionalities, without rising to the level of adopting integrated security strategies. This indicates the need to strengthen the practical dimension of security training.

As for the use of social media platforms, the relative decrease in usage rates may reflect a cautious approach among students in dealing with the digital space. However, this preventative behavior remains insufficient in the absence of advanced technical measures.

Therefore, it can be said that cybersecurity among the studied sample is mostly practiced as specialized knowledge and theoretical understanding, rather than as a comprehensive, daily applied culture. This necessitates a review of training mechanisms to ensure the transformation of knowledge into effective and sustainable preventative practice.

3.Discussion of Results in Light of Previous Studies:

This study aims to examine the relationship between the level of cyber awareness and preventative practices among students at the Higher School of Cybersecurity. The results showed that the sample possesses a considerable level of legal awareness of the risks of cybercrimes, which is reflected in their positive willingness to report digital threats. This finding supports the hypothesis of a positive relationship between awareness and preventative behavior, and it aligns with the results of Vigit's study (2025), which demonstrated a positive correlation between awareness and cybersecurity behaviors.

However, the results also revealed that this awareness is not fully reflected in daily practices. Weaknesses were observed in some basic preventative behaviors, such as regular system updates and limited adoption of advanced protection measures. This finding points to a "knowledge-behavior gap," meaning that knowledge, while important, does not necessarily translate into actionable behavior.

This finding partially aligns with Boochet et al.'s study (2024), which emphasized that awareness alone is insufficient to explain behavior; mediating factors, such as perceived behavioral control, are required. Therefore, the gap observed in the current study can be explained by the weakness of these mediating factors, particularly in the absence of practical training that fosters individuals' confidence in their ability to practice safe behavior. On the other hand, the study's findings align with those of Ben Berghout (2023) and Qashir Saleh (2025), which highlighted challenges in implementing security policies and a lack of digital literacy in Algeria. However, the current study offers a qualitative addition, demonstrating that the problem lies not only in the level of awareness but also in its weak translation into practical practices, even among those academically specialized in cybersecurity.

The results also showed that academic training, despite its specialization, does not necessarily guarantee the acquisition of sustainable preventative behaviors. This coincides with what Qashir Saleh's (2025) study indicated regarding the necessity of developing human competencies. However, the current study clarifies that these competencies should not be limited to the cognitive aspect but should also include the practical and skill-based dimensions.

Therefore, it can be said that the hypothesis concerning a relationship between cybersecurity awareness and preventative behavior has been partially confirmed. The relationship was established at the theoretical level (awareness and preparedness) but was not fully realized at the practical level (actual practice). This confirms that cybersecurity cannot be reduced to knowledge alone, but requires building an applied culture based on continuous training, enhancing practical skills, and providing a learning environment that integrates theory and practice.

VII.Conclusion:

This study sought to explore the level of cybersecurity awareness and practices among a sample of students from the Higher School of Cybersecurity, through the analysis of a set of indicators related to preventive behavior, legal awareness, and the use of digital protection tools. The findings revealed that the participants demonstrated a considerable level of theoretical awareness and legal understanding of cybercrime risks, which was reflected in the high rates of reporting threats and developing certain protection measures. However, the results also revealed a clear gap between theoretical awareness and daily practical application. This was particularly evident in the weak regular updating of systems, the limited adoption of new protection

measures, and the absence of declared practical training in the field of cybersecurity. This paradox acquires particular significance given the specialized nature of the institution to which the participants belong, indicating that academic training, despite its importance, does not necessarily ensure the establishment of systematic and sustainable preventive practices. Accordingly, the study concludes that cybersecurity among the studied sample is practiced more as specialized knowledge than as an everyday applied culture. This highlights the need to reconsider training mechanisms in order to transform theoretical knowledge into effective preventive behavior capable of keeping pace with evolving digital threats.

1. Recommendations:

- Strengthening the practical dimension of academic training by integrating practical training modules that focus on regular system updates, vulnerability management, and the use of advanced protection tools, rather than relying solely on theoretical approaches.
- Establishing a sustainable digital security culture by encouraging students to adopt consistent daily security practices, such as regular updates, systematic encryption, and the use of multi-layered protection solutions.
- Organizing regular training courses and practical workshops within specialized educational institutions to bridge the gap between academic knowledge and the demands of the evolving cybersecurity landscape.
- Enhancing the link between legal awareness and practical behavior by translating legal knowledge of cybercrimes into clear, practical procedures that govern students' daily digital behavior.
- Encouraging further field studies targeting other specialized groups to compare levels of awareness and practice, and to broaden the scientific discussion on cybersecurity issues in academic and professional contexts. Conclusion: This study aimed to explore the level of awareness and practices related to cybersecurity among a sample of students at the Higher School of Cybersecurity, through the analysis of a set of indicators related to preventive behavior, legal awareness, and the use of digital protection tools. The results showed that the participants possessed a considerable level of theoretical awareness and legal understanding of the risks of cybercrime, which was reflected in the high rates of threat reporting and the development of some protection methods.

However, the results also revealed a clear gap between theoretical awareness and daily practical application, particularly manifested in the infrequent updating of systems, the limited adoption of new protection methods, and the absence of formal, accredited training in the field of cybersecurity. This discrepancy is especially significant given the specialized nature of the institution to which the participants belong, indicating that academic training, while important, does not necessarily guarantee the establishment of systematic and sustainable preventive practices.

Therefore, the study concludes that cybersecurity among the studied sample is practiced more as specialized knowledge than as a daily applied culture. This necessitates a rethinking of training mechanisms to allow for the transformation of theoretical knowledge into practical preventative behavior that keeps pace with the evolution of digital threats.

VIII. REFERRALS AND REFERENCES

1. Books

-Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. Educational Planning.

2. Dissertations & Theses

-Abu Hussein, H. (2021). The legal framework for cybersecurity services: A comparative study (Unpublished master's thesis). Faculty of Law, Middle East University, Jordan.

3. Journal Articles

-Al-Saadat, K., & Al-Tamimi, N. (2022). Raising cybersecurity awareness among teachers in light of adult education principles. New Horizons in Adult Education, 1(32).

-Bara, S. (2017). Cybersecurity in Algeria: Policies and institutions. Algerian Journal of Cybersecurity, (4), 259.

-Hantouli, A., & Al-Zaboun, M. (2025). The reality of Jordanian university students' awareness of cybersecurity culture, concepts, and fields from the students' perspective. Al-Manarah Series of Educational and Psychological Sciences, 4(1).

-Haswa, R., & Al-Qudah, M. A. (2023). The role of high school teachers in developing cybersecurity awareness among students from the teachers' perspective in private education schools in Amman. Journal of Educational Science Studies.

-McGregor, R., et al. (2025). Consumer perceptions of personal cyber awareness, knowledge, and risk. Journal of Cybersecurity, 11(1).

-Oudah, H. (2025). Challenges facing cybersecurity. Journal of Humanitarian and Natural Sciences, (6),

4. Internet Websites

-Cybersecurity & Infrastructure Security Agency (CISA). (2025). Cybersecurity Best Practices. Retrieved January 27, 2026, from https://www.cisa.gov/topics/cybersecurity-best-practices.