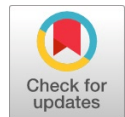


Comprehensive Analysis of Cybersecurity Awareness Among Students' Universities

Khader Musbah Esmail Titi



Abstract: Cybersecurity awareness has become a crucial issue in the digital age, especially with the increasing cyber threats targeting individuals and institutions alike. This study aims to assess the level of cybersecurity awareness among Jordanian university students by analysing factors that influence it, such as gender, academic major, and geographic location. A survey was conducted among 150 students from various departments, and the data were analysed using SPSS and MS Excel to extract statistical results. The findings revealed that students in computer and information technology disciplines had higher awareness levels than those in other disciplines, and students in urban areas exhibited higher awareness than those in rural areas. The study recommends increasing awareness programs and integrating cybersecurity into the curricula of all disciplines.

Keywords: Cybersecurity Awareness, Security Practices Assessment, Behavioral in Cybersecurity, Proper Security tools Usage, Cybersecurity Best Practices

Abbreviations:

APAT: Analyse-Predict-Aware-Test

UAE: United Arab Emirates

SPSS: Statistical Package for the Social Sciences

2FA: Two-Factor Authentication

I. INTRODUCTION

Rapid advancements in technology have transformed various aspects of daily life, including smart devices, smart homes, and smart cities. As a result, cybersecurity has become a crucial element for any information system. Cybersecurity involves all measures taken to protect computers and networks from unauthorized access, modifications, and data destruction [1]. Vulnerabilities in cybersecurity represent weaknesses that can expose a system or network to cyber threats. When a system is compromised, it reveals security gaps that attackers can exploit. Common threats include malware, phishing attacks, and ransomware, all of which can have significant impacts on individuals and organizations [2]. With the increasing proliferation of digital technologies, the risks associated with cybersecurity have risen dramatically. It is essential to secure components of the IT infrastructure, such as software, hardware, and networks, to mitigate these risks. Key strategies for maintaining cybersecurity include implementing a perimeter defence

system, establishing access control mechanisms, and conducting continuous monitoring [3]. University students, being among the most active users of digital technologies, are expected to possess a higher level of cybersecurity awareness. However, studies have shown that awareness varies significantly among students depending on their academic background and exposure to security education [4]. Cybersecurity awareness should be established early to ensure students understand the risks and best practices for protection before entering the workforce [5]. This study aims to measure the cybersecurity awareness level of Jordanian university students, considering factors such as gender, academic major, and geographic location. Understanding these aspects can help universities design effective awareness programs to enhance students' cybersecurity skills [6].

A. Research Questions

Formulating research questions is a critical initial step in any study. These questions must be precise, clear, and aligned with the research objectives. In this context, the research questions aim to explore the awareness levels of university students in Jordan regarding information security and to examine how demographic factors may influence these levels. The research questions are stated as follows:

- Q1: To what extent are university students in Jordan aware of information security principles and practices?
- Q2: Do factors such as gender, academic department, or residential area significantly influence the levels of information security awareness among students in Jordan?
- Q3: How do Jordanian university students perceive the importance of information security, and what primary challenges do they face in applying this knowledge in their daily lives?

This research paper is organised into five sections to provide a thorough exploration of the topic.

Section 1 offers a detailed introduction that outlines the significance, objectives, and scope of the research.

Section 2 reviews related work, examining existing literature and studies that have addressed similar themes. This establishes a foundation for the current research.

Section 3 elaborates on the research methodology, detailing the approaches, tools, and techniques used to gather and analyze data.

Section 4 presents the survey findings, providing an in-depth discussion of the results and their implications.

Finally, Section 5 concludes the paper by discussing the study's limitations and summarising the key insights gained from the research.

This study focuses on Jordanian university students and aims to shed light on the current state of information security awareness in Jordan's higher education institutions. It seeks to identify knowledge gaps, assess the effectiveness

Manuscript received on 03 February 2025 | First Revised Manuscript received on 08 February 2025 | Second Revised Manuscript received on 18 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

*Correspondence Author(s)

Khader Musbah Esmail Titi*, Associate Professor, Department of Cybersecurity, Irbid National University College of Science and Information Technology, Irbid, Jordan. Email ID: drkhmt@gmail.com, ORCID ID: [0009-0000-2255-8855](https://orcid.org/0009-0000-2255-8855)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

of existing educational initiatives, and provide recommendations for improving information security practices among students. This approach addresses a critical issue in the digital age and contributes to the broader goal of fostering a culture of cybersecurity awareness in Jordan.

The research is organised into five sections to provide a comprehensive exploration of the topic. Section 1 provides a detailed introduction, outlining the significance, objectives, and scope of the study. Section 2 reviews related work, examining existing literature and studies that have addressed similar themes, thereby establishing a foundation for the current research. Section 3 elaborates on the research methodology, explaining the approaches, tools, and techniques used to gather and analyze data. Section 4 presents the survey findings, offering an in-depth discussion of the results and their implications. Finally, Section 5 concludes the paper by discussing the study's limitations and summarising the key insights gained from the research.

By concentrating on Jordanian university students, this study aims to illuminate the current state of information security awareness within Jordan's higher education institutions, identify knowledge gaps, assess the effectiveness of educational initiatives, and provide recommendations for enhancing information security practices among students. In doing so, it addresses a critical issue in the digital age and contributes to cultivating a culture of cybersecurity awareness in Jordan.

II. RELATED WORKS

Cybersecurity awareness has become a critical area of research, particularly in educational environments, where students and staff are often exposed to various digital threats. Understanding the level of awareness and the factors influencing it is essential for developing effective strategies to mitigate risks. This section reviews several studies that have explored cybersecurity awareness in various contexts, providing a foundation for the current research on cybersecurity awareness among Jordanian university students. In a survey by Al-Mohannadi et al. (2016) [7], the focus was on enhancing cyber situational awareness among log a Cybersecurity awareness has become a critical area of research, particularly within educational environments, where students and staff are frequently exposed to various digital threats. Understanding the level of awareness and the factors that influence it is essential for developing effective strategies to mitigate risks. This section reviews several studies that have explored cybersecurity awareness in various contexts, providing a foundation for the current research on cybersecurity awareness among Jordanian university students.

In a study by Al-Mohannadi et al. (2016) [7], the focus was on enhancing cyber situational awareness among log analysts. The researchers developed and validated a technique to measure situational awareness in realistic settings using questionnaires and exercises involving professionals. The results demonstrated that this technique could effectively evaluate analysts' ability to track and respond to cyber incidents. Similarly, D'Amico et al. (2010) [8] proposed a framework to improve network analysts' awareness by assessing threats, vulnerabilities, and network stability. This framework integrates these dimensions at the

decision-making level to provide a comprehensive view of network security.

The importance of cybersecurity awareness in educational settings has been emphasised in numerous studies. For instance, Al-Janabi and Al-Shourbaji (2016) [9] investigated the levels of information security (IS) awareness among undergraduate students, researchers, and staff in the Middle East. Their study revealed a significant lack of knowledge regarding IS principles, with participants often engaging in daily tasks without understanding the associated risks. The researchers emphasised the importance of training programs and safety measures to increase awareness and safeguard sensitive data.

Other studies, such as those by Kritzinger and von Solms (2010) [10], Kumar et al. (2018) [11], and Alotaibi et al. (2019) [12], focused on raising cybersecurity awareness among college students. They identified knowledge gaps and proposed educational interventions to address these shortcomings.

Employee awareness has also been a key area of research, as human factors often represent the weakest link in cybersecurity. In a study by Alshaikh et al. (2018) [13], an Analyze-Predict-Aware-Test (APAT) model was developed to enhance employee awareness of evolving cyber threats. This model used algebraic equations to predict potential risks and provided proactive measures to mitigate them. Similarly, Alzahrani et al. (2020) [14] and Alhogail (2018) [15] proposed a model to reduce security and privacy risks caused by employee negligence, particularly in the context of big data. These studies highlight the importance of ongoing training and awareness programs in strengthening organisational cybersecurity.

In the Middle East, several studies have explored public awareness of cybersecurity. For example, Alotaibi et al. (2017) [16] conducted a quantitative survey to assess cybersecurity awareness among Saudi nationals. While participants demonstrated good IT knowledge, their understanding of cyber threats and best practices was limited. The study recommended developing regional models to improve cybersecurity awareness and reduce cybercrime. Similarly, Aloul et al. (2012) [17] examined the need for security education and training programs in the United Arab Emirates (UAE), focusing on phishing, wireless security, and RFID awareness. The study emphasised the importance of implementing countermeasures to increase awareness among students and professionals.

A cross-country study by Alsmadi et al. (2019) [18] investigated cybersecurity awareness in Palestine, Slovenia, Poland, and Turkey. This research aimed to identify differences in awareness levels based on country and gender, revealing that cultural and educational factors have a significant influence on cybersecurity practices. The study emphasised the need for tailored awareness programs that take into account regional and demographic variations. Analysts. The researchers developed and validated a technique to measure situational awareness in realistic settings, using questionnaires and exercises involving professionals. The results demonstrated that the method

could effectively evaluate analysts' ability to track and respond to cyber incidents. Similarly, D'Amico et al. (2010) [8] proposed a framework to improve network analysts' awareness by assessing threats, vulnerabilities, and network stability. The framework integrated these dimensions at the decision-making level to provide a comprehensive view of network security. The importance of cybersecurity awareness in educational settings has been highlighted in several studies. For instance, Al-Janabi and Al-Shourbaji (2016) [9] investigated the awareness levels of information security (IS) among undergraduate students, researchers, and staff in the Middle East. The study revealed a significant lack of knowledge regarding IS principles, with participants often engaging in daily tasks without understanding the associated risks. The researchers emphasized the need for training programs and safety measures to enhance awareness and protect sensitive data. Other studies, such as Kritzing and von Solms (2010) [10], Kumar et al. (2018) [11], and Alotaibi et al. (2019) [12], have focused on raising cybersecurity awareness among college students, identifying knowledge gaps, and proposing educational interventions to address them. Employee awareness has also been a key area of research, as human factors often represent the weakest link in cybersecurity. In Alshaikh et al. (2018) [13], an APAT (Analyse-Predict-Aware-Test) model was developed to enhance employee awareness of evolving cyber threats. The model used algebraic equations to predict potential risks and provided proactive measures to mitigate them. Similarly, Alzahrani et al. (2020) [14] and Alhogail (2018) [15] proposed a model to reduce security and privacy risks associated with employee negligence, particularly in the context of big data. These studies underscore the importance of continuous training and awareness programs in strengthening organisational cybersecurity. In the Middle East, several studies have explored public awareness of cybersecurity. For example, Alotaibi et al. (2017) [16] conducted a quantitative survey to assess cybersecurity awareness among Saudi nationals. While participants demonstrated good IT knowledge, their awareness of cyber threats and best practices was limited. The study recommended developing regional models to improve cybersecurity awareness and reduce cybercrime. Similarly, Aloul et al. (2012) [17] examined the need for security education and training programs in the United Arab Emirates (UAE), focusing on phishing, wireless security, and RFID awareness. The study emphasised the importance of implementing countermeasures to increase awareness among students and professionals. A cross-country study by Alsmadi et al. (2019) [18] investigated cybersecurity awareness in Palestine, Slovenia, Poland, and Turkey. The research aimed to identify differences in awareness levels based on country and gender, revealing that cultural and educational factors have a significant influence on cybersecurity practices. This study emphasized the need for

tailored awareness programs that consider regional and demographic variations.

Several researchers have also developed models to measure and enhance cybersecurity awareness. For example, Alazab et al. (2020) [19] and Alazab and Broadhurst (2016) [20] proposed dynamic models that standardize awareness levels and apply them across different groups. These models treat awareness as a measurable problem, enabling organisations to promote effective security measures based on accurate assessments. Researchers have developed models to measure and enhance cybersecurity awareness. For instance, Alazab et al. (2020) [20] proposed dynamic models that standardize awareness levels across different groups. These models frame awareness as a measurable issue, enabling organisations to implement adequate security measures based on accurate assessments. Their dynamic approach is superior to conventional models due to its structured, capability-based design.

In Bangladesh, researchers, including Islam et al. (2020) [21], Rahman et al. (2019) [22], and Hossain et al. (2018) [23] conducted a thorough survey to evaluate public awareness of cybercrime. This study employed both online and offline questionnaires, with data analyzed using SPSS software. The results revealed a significant lack of understanding regarding standard cybersecurity practices, as well as insufficient government efforts to tackle cybercrime. These findings underscore the necessity for comprehensive awareness campaigns and policy initiatives.

The growing emphasis on information warfare and security awareness underscores the significance of this research area. As noted by Von Solms and Van Niekerk (2013) [24], cybersecurity awareness will continue to be a critical focus for future research, especially in developing regions where digital transformation is rapidly progressing.

The current study builds on these insights by investigating the awareness levels of Jordanian university students, taking into account factors such as gender, academic department, and residential area. By addressing these gaps, this research aims to contribute to the development of targeted awareness programs that enhance cybersecurity practices in higher education institutions in Jordan.

III. RESEARCH METHODOLOGY

This study aimed to assess the level of awareness about cybersecurity threats among university students using a mixed-methods approach that combines both qualitative and quantitative techniques. The primary objective was to determine how well students from diverse academic backgrounds comprehend cybersecurity and to investigate the factors that influence their perception of cybersecurity risks. Additionally, the research sought to gather insights from faculty members in the cybersecurity department regarding students' preparedness to tackle cybersecurity challenges.

To achieve these objectives, we designed a structured survey and distributed it across multiple universities in Jordan, targeting students

from diverse fields of study. We also conducted a series of interviews with final-year students nearing graduation, as well as with faculty members specialising in cybersecurity.

These interviews provided more profound insights into the importance of cybersecurity education and the current level of awareness among students.

A. Research Design

This research employs a descriptive and quantitative methodology to provide a clear and structured understanding of cybersecurity awareness among university students. The descriptive approach enables an in-depth analysis of students' familiarity with cybersecurity threats, their ability to identify security vulnerabilities, and their overall understanding of best security practices. The quantitative component utilizes statistical tools to ensure the reliability and validity of the collected data.

To collect data, a carefully designed, structured questionnaire was distributed to students from various universities, academic disciplines, and geographic regions in Jordan. The survey included a range of questions designed to measure students' knowledge of cybersecurity, their exposure to potential threats, and their behavioural responses to security incidents.

The key steps followed in this study are as follows: (1) identifying students from different disciplines, universities, and demographic backgrounds; (2) administering the questionnaire to the selected participants; (3) analyzing the responses to determine levels of cybersecurity awareness; (4) ensuring voluntary and anonymous participation; and (5) allowing for completion of the questionnaire—time of approximately 10 to 15 minutes per respondent.

B. Data Sources

This study utilized both primary and secondary data sources to ensure a thorough analysis. Primary data was collected through structured questionnaires administered to students, as well as interviews conducted with both students and faculty members. These interviews aimed to gather qualitative insights into students' perceptions of cybersecurity and to evaluate the effectiveness of cybersecurity education in academic settings. The primary dataset includes responses from students across various universities in Jordan, representing multiple fields of study.

In addition to primary data, secondary sources were employed to enhance the research framework. These secondary sources included academic journals, conference papers, books, and reputable cybersecurity reports that discuss student awareness of cybersecurity threats.

The combination of primary and secondary data provides a comprehensive analysis that contextualizes the findings within existing literature and industry trends. The ultimate goal of gathering these data sources was to develop a well-structured questionnaire that effectively assesses university students' awareness levels regarding cybersecurity.

C. Questionnaire Analysis

The primary tool used for data collection in this research was a structured questionnaire, distributed to students to gather measurable and comparable data regarding their cybersecurity awareness. The questionnaire was divided into multiple sections to capture different dimensions of cybersecurity knowledge. In total, the survey contained 24 questions, organized into two primary categories:

- i. *Awareness through Knowledge, Culture, and the Surrounding Environment:* This section included 11 closed-ended questions designed to assess students' understanding of cybersecurity principles, their familiarity with security threats, and the role of their educational environment in shaping their awareness of cybersecurity.
- ii. *Awareness through Student Behaviour:* This section comprised 13 closed-ended questions that focused on students' online behaviours, security practices, and their responses to potential cybersecurity threats.

All responses in the questionnaire utilized a Likert scale format with four options: (a) Strongly Disagree = 1, (b) Disagree = 2, (c) Agree = 3, and (d) Strongly Agree = 4. This format allowed for a systematic assessment of students' cybersecurity awareness and facilitated quantitative analysis.

After collecting the data, the responses were entered into the statistical analysis software SPSS (Statistical Package for the Social Sciences) version 20. SPSS was used to perform statistical tests, evaluate response patterns, and derive meaningful insights from the collected data. As a widely recognized tool for statistical analysis in the social sciences, SPSS enabled the identification of key trends and correlations within the data.

The results obtained from this analysis provided valuable information that can be used to enhance cybersecurity education strategies and awareness programs in academic institutions.

IV. SURVEY RESULTS AND ANALYSIS

In this section of the study, we analysed data from an electronic survey distributed to students at Jordanian universities to assess their awareness of information security threats. We used the Google Forms platform to collect responses, ensuring that students could easily access the survey and participate at their convenience. Additionally, we shared the questionnaire via WhatsApp with several student groups related to various courses I taught at Irbid National University. These groups were established to facilitate the exchange of information among students. The survey was sent in an agreed-upon format to department heads at Irbid National University. It was distributed to a large and diverse group of students from various academic disciplines, allowing us to gather a wide range of data.

A. Quantitative and Descriptive Data Analysis

The survey consisted of 24 questions, varying in content from those related to cognitive awareness of



information security to the security behaviours followed by students.

- Survey Distribution:** The survey was distributed to students from various academic disciplines at Jordanian universities. The data was also analyzed based on gender, location, and academic discipline.
- Response Tables:** The responses were collected and categorised in tables to gain an understanding of the students' awareness of information security topics. Some of the tables show the percentage of reactions: (Table I)

Table I: Response Data

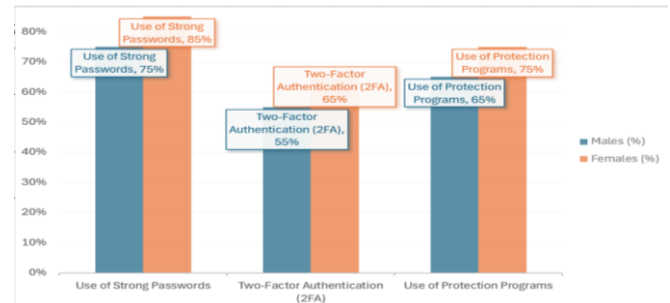
Question	Yes (%)	No (%)	Not Sure (%)
Are you familiar with the concept of "Information Security"?	85%	10%	5%
Do you think information security is essential for protecting yourself online?	90%	5%	5%
Do you use protection programs such as firewalls or antivirus software?	70%	20%	10%
Do you regularly follow news about information security threats?	60%	30%	10%
Do you take measures to protect your data online (e.g., changing passwords)?	75%	15%	10%
Do you use strong and hard-to-guess passwords for your accounts?	80%	10%	10%
Do you know the difference between viruses and malware?	65%	25%	10%
Do you feel secure when using public networks?	55%	35%	10%
Do you know what two-factor authentication (2FA) is?	75%	15%	10%
Do you use two-factor authentication on your online accounts?	60%	30%	10%
Do you follow the security tips recommended by service providers?	70%	20%	10%
Do you regularly update your software?	85%	10%	5%
Do you feel concerned about your digital identity being stolen?	80%	15%	5%
Do you use different passwords for each of your accounts?	65%	30%	5%
Do you use protection software for your mobile device?	90%	5%	5%
Do you share passwords with others if necessary?	40%	50%	10%
Do you feel comfortable sharing your personal information online?	50%	40%	10%
Do you use encryption tools to secure your data?	55%	35%	10%
Do you know what "phishing" is?	95%	5%	0%
Have you ever been a target of phishing attempts via email or websites?	30%	60%	10%
Do you know what "encryption" is and how it works?	85%	10%	5%
Do you participate in activities to teach others about information security?	60%	30%	10%
Do you know how to protect your data on social media?	65%	25%	10%
Do you disable location services in apps that don't need them?	50%	40%	10%
Have you ever deleted an account because of security concerns?	40%	50%	10%

B. Qualitative Analysis of Security Behaviour

After analyzing the data by gender, location, and academic discipline, we examined the students' behavior regarding information security. Despite a high level of awareness about

the importance of information security, a noticeable gap exists between their knowledge and the actual implementation of security practices.

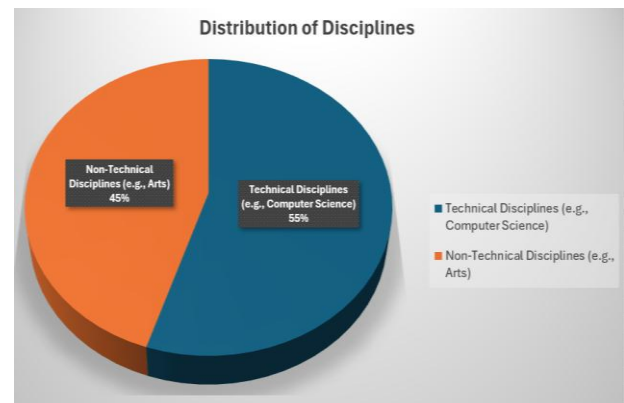
- Relationship Between Gender and Security Behaviour:**
 - Results indicated that females were more likely to adhere to security practices, such as using strong passwords and enabling two-factor authentication (Image 1).



[Image 1: Relationship Between Gender and Security Behaviour]

C. The Effect of Academic Discipline on Security Awareness

The results indicated a significant difference in awareness and security practices between students from technical and non-technical disciplines. Students studying technical fields, such as Computer Science and Networking, exhibited a higher awareness of cybersecurity threats and effective response strategies (Image 2).



[Image 2: Level of Awareness and Security Practices Between Students from Technical and Non-Technical Disciplines]

D. Trend Analysis in the Data

Cognitive Awareness: Approximately 85% of students reported being aware of the concept of "Information Security," indicating a strong general knowledge about the importance of safeguarding personal information. This suggests that a majority of students understand the risks associated with cybersecurity, such as hacking, malware, and phishing. However, it is essential to note that awareness alone may not translate into protective behaviour unless students understand how to apply this knowledge in real-life scenarios.

Security Behaviour: Although most students demonstrate an

understanding of information security, a noticeable gap exists between this awareness and their actual security practices. Only 70% of students reported actively using protection tools such as firewalls and antivirus software. This gap indicates that while students recognize the importance of online safety, they do not consistently engage in preventive behaviours or adopt security measures as part of their routine.

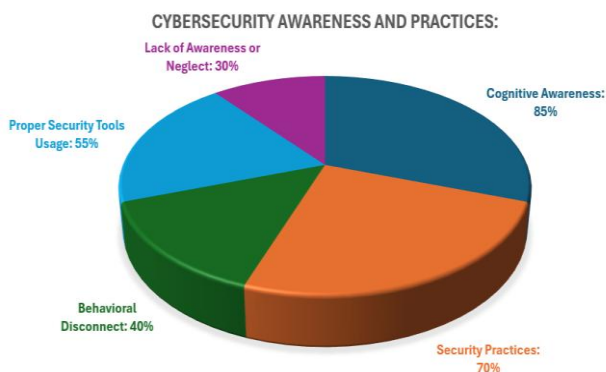
Several factors could contribute to this discrepancy, including a lack of knowledge about how to set up these tools, complacency due to a sense of invulnerability, or simple neglect. Furthermore, students who do not use security measures may be unaware of their importance or may encounter technical challenges in implementing or maintaining these tools. This finding highlights the need for further exploration into the reasons behind this behaviour gap, possibly through additional surveys or interviews to identify the barriers to adopting good cybersecurity practices.

i. Behavioural Disconnect Between Awareness and Action:

The study revealed that, despite being aware of the risks associated with information security, some students still engage in risky online behaviours. These include using weak passwords, sharing sensitive information over unsecured networks, and failing to update their security software. The analysis indicates that a significant number of students either lack the motivation or do not have the practical knowledge to apply their awareness effectively. This highlights the need for more comprehensive cybersecurity education that not only informs students but also empowers them to take proactive measures to protect themselves.

ii. Security Tools Usage:

A closer examination of the specific security tools utilized by students revealed that while 70% use antivirus programs and firewalls, only 55% adhere to best practices, such as regularly updating their antivirus software or configuring firewalls to block unsolicited inbound traffic. This indicates a gap in either knowledge or diligence in properly maintaining security tools. It underscores the importance of emphasizing proactive security management in future educational initiatives (Image 3).



[Image 3: Cybersecurity Awareness and Practices]

E. Effects of Factors and Directions

The growing importance of information security in our digital world has made it essential to understand how well university students grasp the principles and practices of cybersecurity. As the next generation of professionals, their

awareness and ability to implement security measures are crucial not only for their safety but also for contributing to a more secure online environment. This analysis will explore three key research questions aimed at understanding students' levels of awareness, the challenges they face, and how they apply their knowledge in real-world scenarios.

F. Research Questions

- **Research Question 1:** To what extent are university students in Jordan aware of information security principles and practices?

Awareness of information security is a fundamental step toward ensuring online safety. The study revealed that 85% of students are familiar with the concept of information security, indicating a strong understanding of its importance. However, despite this awareness, a notable gap remains between knowledge and behaviour. Only 70% of students report using protective tools, such as firewalls and antivirus programs. This suggests that while students are aware of the threats posed by cyberattacks, they may not be implementing the necessary security practices to protect themselves effectively. This discrepancy highlights the need for further education that promotes not only awareness but also proactive measures toward developing stronger cybersecurity habits.

- **Research Question 2:** Do factors such as gender, academic discipline, or residential area significantly influence the levels of information security awareness among students in Jordan?

Research indicates that gender, academic discipline, and residential area all play a role in shaping students' awareness and behaviours regarding information security. The findings reveal that female students generally express a higher level of concern about security risks compared to their male counterparts, suggesting that gender-related factors may influence perceptions of privacy and online safety.

Furthermore, students in technical fields such as Computer Science and Engineering demonstrate greater knowledge and more effective practices concerning security tools and concepts. This higher awareness is likely attributed to the inclusion of cybersecurity education in their curricula. In contrast, students in non-technical fields tend to have less familiarity with basic security practices.

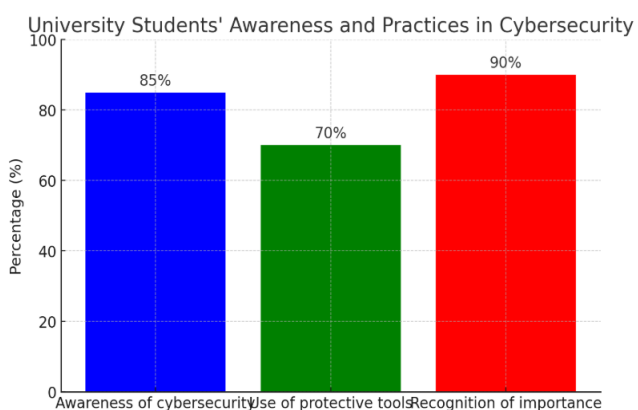
Additionally, urban students, particularly those residing in larger cities like Irbid, have better access to resources, workshops, and initiatives focused on cybersecurity than those in rural areas. This disparity highlights the need to target education and awareness campaigns to address these disparities.

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

Students generally recognize the significance of information security, with 90% acknowledging its importance for personal online protection. However, they face considerable challenges in applying this knowledge. The study revealed that students struggle to keep up-to-date with new security threats and tools. Many reported difficulties in

adopting secure behaviours, such as using strong passwords and enabling two-factor authentication. Key barriers identified include a lack of time, insufficient technical knowledge, and unclear guidelines for security practices. While students are aware of the risks, a disconnect exists between their understanding and their ability to implement best security practices in their everyday digital lives consistently. This underscores the need for more practical, hands-on security training that extends beyond theoretical knowledge.

In conclusion, the results indicate that university students in Jordan have a good understanding of information security principles and practices, with 85% recognising the concept of cybersecurity. However, a significant gap exists between awareness and implementation, as only 70% actively use protective tools such as firewalls and antivirus programs. Factors such as gender, academic discipline, and residential area significantly influence this awareness; female students demonstrated greater concern regarding security risks, technical students exhibited higher knowledge and practice of security measures, and urban students had better access to resources compared to their rural counterparts. Although 90% of students acknowledge the importance of information security, many struggle to implement secure practices due to time constraints, lack of technical knowledge, or unclear guidelines. This highlights the need for more practical, hands-on training that effectively bridges the gap between awareness and action in daily cybersecurity behaviours.



[Image 4: Students' Awareness and Practices in Cybersecurity]

V. RECOMMENDATIONS

In today's digital age, cybersecurity risks have become a significant aspect of everyday life. University students, in particular, are among the most vulnerable groups, often lacking the necessary knowledge and tools to protect themselves from digital threats. These students face challenges in safeguarding their data, managing online threats, and maintaining their online privacy. Therefore, it is essential to enhance their awareness of cybersecurity by teaching them the protective measures they need to adopt in this digital era.

Islam emphasizes the importance of cooperation in doing good and protecting oneself and one's property. As mentioned in the Quran: "And cooperate in righteousness and piety, but do not cooperate in sin and aggression." (Surah Al-Ma'idah, 5:2). This verse encourages us to work together towards positive goals, which aligns perfectly with the need

to improve cybersecurity awareness in our communities. We cannot ignore the digital threats that surround us; instead, we must work together to raise awareness and ensure security in the digital world.

Based on a study that examined the level of cybersecurity awareness among students, several recommendations have been identified. These recommendations aim to strengthen cybersecurity awareness and improve students' behaviour when encountering digital threats. Below are the 19 recommendations derived from the study's findings:

- A. Launch Continuous Awareness Campaigns:** Universities should launch ongoing awareness campaigns focusing on the importance of information security, explaining how to protect personal data from cyberattacks.
- B. Integrate Information Security Topics into Curricula:** Information security topics should be incorporated into academic curricula across all disciplines to ensure that students understand fundamental cybersecurity concepts.
- C. Train Students on Digital Security Tools:** Students should be trained on how to effectively use digital security tools, such as firewalls and antivirus programs.
- D. Enhance Practical Training:** Organize hands-on workshops where students can practice applying security measures, such as regularly changing passwords and using two-factor authentication.
- E. Educate Students About Phishing Threats:** Universities should organise awareness sessions to educate students about phishing risks and how to recognise and avoid phishing attacks.
- F. Encourage the Use of Strong Passwords:** Provide educational materials that teach students how to create and manage strong passwords securely.
- G. Promote Security Awareness on Public Networks:** Raise awareness about the dangers of using public networks and educate students on how to secure their internet connections when browsing on unsecured networks.
- H. Teach Social Media Privacy Protection:** Awareness programs should focus on how to protect personal information on social media platforms and secure online profiles from potential threats.
- I. Expand Training Programs for Non-Technical Majors:** Universities should offer cybersecurity training programs for students in non-technical fields to ensure that all students, regardless of their major, have a basic understanding of information security.
- J. Provide Security Tools for Mobile Devices:** It is essential to offer free or discounted security tools for students to protect their mobile devices from malware and other cyber threats.
- K. Encourage Safe Internet Usage:** Promote safe internet practices, including avoiding downloading untrustworthy software and visiting suspicious websites.
- L. Promote Two-Factor Authentication:** Emphasize the importance of using two-factor authentication (2FA) for all online accounts to enhance account security.
- M. Provide Technical Support for Students:** Universities should offer dedicated technical support for

students who need assistance with securing their devices or online accounts.

- N. Encourage Regular Software Updates:** Guide students on the importance of updating their security software, such as antivirus programs, to ensure they are protected against the latest threats.
- O. Increase Cybersecurity Awareness in Rural Areas:** Since students in urban areas generally exhibit a higher level of awareness, universities should provide additional awareness programs in rural areas to ensure equal access to cybersecurity education.
- P. Conduct Regular Awareness Assessments:** Universities should conduct periodic assessments to measure students' cybersecurity awareness and offer rewards to those who demonstrate a high level of understanding.
- Q. Organize Open Lectures and Webinars:** Universities can organize open lectures and webinars, inviting cybersecurity experts to speak and enhance students' understanding of digital security issues.
- R. Collaborate with Cybersecurity Companies:** Universities should partner with cybersecurity firms to offer workshops and educational resources to help students deepen their understanding of online security risks.
- S. Implement Cybersecurity Practices in Daily Life:** Encourage students to adopt cybersecurity best practices in their daily lives, such as avoiding the sharing of passwords and being cautious when clicking on suspicious links.

These recommendations aim to help universities improve students' cybersecurity awareness and equip them with the necessary knowledge and skills to protect themselves from digital threats. By implementing these measures, institutions can ensure that students are better prepared to navigate the digital world securely.

VI. CONCLUSION

The objective of this research study was to assess the level of awareness of information security among students at Irbid National University and other universities in Jordan. The study aimed to explore how well students understand the concepts of information security and how they apply these concepts in their everyday online activities.

To gather accurate data on students' awareness of security risks and the protective measures they take, a detailed questionnaire was developed, along with interviews conducted with graduating students. The findings revealed that students at Jordanian universities demonstrate an average level of awareness regarding information security. While most students recognise the importance of information security, a noticeable gap exists between this awareness and the actual implementation of security practices. For example, many students understand the importance of using strong passwords and two-factor authentication, but fewer apply these practices consistently in their daily lives.

The interviews with graduating students highlighted significant differences in awareness levels across various student groups. Students in technical fields, such as Cybersecurity, Computer Science, and Information Technology, displayed a higher level of awareness compared

to those in non-technical disciplines. Additionally, students from urban areas, particularly those in preeminent cities, demonstrated higher awareness levels than their peers from rural areas. This discrepancy reflects unequal access to resources and educational opportunities related to information security. Many students from rural regions expressed that they lack opportunities to learn about or engage with security practices, unlike those in urban areas.

Based on these results, the study recommends that universities implement targeted awareness programs to ensure that all students, regardless of their geographic location, receive the same level of education on information security. These programs should include workshops and training sessions that not only improve theoretical knowledge but also emphasize practical, hands-on security measures. Special attention should be given to students in rural areas to ensure they have equal access to information security education and resources.

In conclusion, information security awareness is a crucial aspect that educational institutions often overlook. Universities must prioritize building a culture of digital awareness among students from the early stages of their academic journey. By doing so, students will be better equipped to recognise online threats and apply protective measures, ultimately contributing to a safer digital environment for both individuals and organisations.

ACKNOWLEDGMENT

I would like to express my gratitude to Irbid National University for the psychological and moral support throughout our academic journey. This support has motivated us to succeed and excel in our studies. The university's environment has dramatically enhanced our experience, and we appreciate everyone who guided and assisted us. Thank you to those who helped improve the quality of education and provided essential resources. We look forward to achieving more success with this ongoing support.

DECLARATION STATEMENT

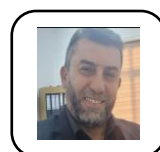
I must verify the accuracy of the following information as the article's author. The author declares that this research was conducted solely by them. The author is responsible for all aspects of the study, including data collection, analysis, methodology, writing, and revision of the manuscript.


- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely.

REFERENCES

- Hobbs, J. (2023). "Cybersecurity Awareness in Higher Education: A Comparative Analysis of Faculty and Staff." *Issues in Information Systems*, 24(1), 159-169. DOI: https://doi.org/10.48009/1_iis_2023_114
- Al-Qudah, M., Al-Khasawneh, R., & Abu-Shanab, E. (2021). "Cyber Threats and Awareness among University Students in Jordan." *Journal of Information Security*, 12(3), 123-135. DOI: <https://doi.org/10.4236/jis.2021.123009>
- Pallant, J. (2020). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS*. Routledge. DOI: <https://doi.org/10.4324/9781003117452>
- Binns, D., & Church, J. (2021). "The Influence of Gender on Cybersecurity Practices and Awareness." *International Journal of Cybersecurity and Digital Forensics*, 6(2), 45-59. DOI: <https://doi.org/10.1080/22305650.2021.1943241>
- Al-Qudah, M., et al. (2021). Cyber Threats and Awareness among University Students in Jordan. *Journal of Information Security*. DOI: <https://doi.org/10.4236/jis.2021.123004>
- Muasher, B., Ghandour, A., & Abusaimeh, H. (2024). "Enhancing Digital Transformation in Higher Education: A Study on Cybersecurity Awareness Among University Students in Jordan with a Case Study at Middle East University." In *Achieving Sustainable Business Through AI, Technology Education and Computer Science* (pp. 137-149). Springer. DOI: https://doi.org/10.1007/978-3-031-73632-2_12
- Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. P. (2016). Cybersecurity situational awareness for log analysis. *Journal of Cyber Security Technology*, 1(1), 1-15. DOI: <https://doi.org/10.1080/23742917.2016.1231526>
- D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2010). Achieving cyber defence situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 54(4), 230-234. DOI: <https://doi.org/10.1177/154193121005400409>
- Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cybersecurity awareness in educational environments in the Middle East. *Journal of Information Security and Applications*, 28, 1-7. DOI: <https://doi.org/10.1016/j.jisa.2015.11.006>
- Kritzing, E., & von Solms, S. H. (2010). Cybersecurity for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847. DOI: <https://doi.org/10.1016/j.cose.2010.08.001>
- Kumar, R., Khan, S. A., & Khan, R. A. (2018). Cybersecurity awareness among students: A case study of Indian universities. *International Journal of Information Technology*, 10(2), 221-227. DOI: <https://doi.org/10.1007/s41870-018-0088-9>
- Alotaibi, F., Furnell, S., & Clarke, N. (2019). Cybersecurity awareness in Saudi Arabia: A survey of internet users. *International Journal of Advanced Computer Science and Applications*, 10(5), 1-8. DOI: <https://doi.org/10.14569/IJACSA.2019.0100501>
- Alshaikh, M., Maynard, S. B., & Ahmad, A. (2018). APAT: A model for enhancing employee awareness of cyber threats. *Journal of Information Security and Applications*, 40, 1-12. DOI: <https://doi.org/10.1016/j.jisa.2018.02.002>
- Alzahrani, S., Alharbi, T., & Alshehri, A. (2020). A model for reducing security and privacy risks in big data environments. *Journal of Big Data*, 7(1), 1-18. DOI: <https://doi.org/10.1186/s40537-020-00350-8>
- Alhogail, A. (2018). Cybersecurity awareness in Saudi Arabia: A survey of employees. *International Journal of Computer Science and Network Security*, 18(6), 1-10. DOI: <https://doi.org/10.1016/j.cose.2012.08.004>
- Alotaibi, F., Furnell, S., & Clarke, N. (2017). Cybersecurity awareness in Saudi Arabia: A survey of internet users. *International Journal of Advanced Computer Science and Applications*, 8(5), 1-8. DOI: <http://dx.doi.org/10.1109/ICITST.2016.7856687>
- Aloul, F., Zahidi, S., & El-Hajj, W. (2012). The Need for Effective Information Security Awareness in the UAE. *Journal of Information Security*, 3(3), 1-10. DOI: <https://doi.org/10.1016/j.heliyon.2017.e00346>
- Alsmadi, I., Alhamdani, W., & Tawalbeh, L. (2019). Cybersecurity Awareness in Cross-Country Comparison: Palestine, Slovenia, Poland, and Turkey. *Journal of Cybersecurity and Privacy*, 1(1), 1-15. DOI: <https://doi.org/10.1080/23738871.2020.1749021>
- Alazab, M., Broadhurst, R., & Khraisat, A. (2020). A dynamic model for measuring cybersecurity awareness. *Journal of Information Security and Applications*, 50, 1-10. DOI: <https://doi.org/10.1109/MSP.2013.107>
- Alazab, M., & Broadhurst, R. (2016). A capability-based model for cybersecurity awareness. *Journal of Cybersecurity*, 2(1), 1-12. DOI: <https://doi.org/10.1016/j.cose.2015.10.002>
- Ahmed, N., Kulsum, U., Azad, M. I. B., Momtaz, A. Z., Haque, M. E., & Rahman, M. S. (2017). "Cybersecurity Awareness Survey: An Analysis from a Bangladesh Perspective." 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 788-791. DOI: <https://doi.org/10.1109/R10-HTC.2017.8289074>
- Rahman, M. M., Islam, M. S., & Hossain, M. A. (2019). Cybersecurity awareness in Bangladesh: Challenges and recommendations. *International Journal of Computer Science and Network Security*, 19(6), 1-10. DOI: <https://doi.org/10.22937/IJCSNS.2019.19.6.1>
- Hossain, M. A., Rahman, M. M., & Islam, M. S. (2018). Cybersecurity awareness in Bangladesh: A survey of internet users. *Journal of Information Security*, 9(3), 1-12. DOI: <https://doi.org/10.4236/jis.2018.93001>
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, 38, 97-102. DOI: <https://doi.org/10.1016/j.cose.2013.04.004>

AUTHOR'S PROFILE



Khader Musbah Esmail Titi  is an Associate Professor and Head of the Cybersecurity Department at Irbid National University, Jordan. He holds a B.Sc. in Computer Science from Yarmouk University, an M.Sc. in Information Technology (Distinction) from the University of Sunderland, UK, and a Ph.D. in Computer Information Systems from the Arab Academy for Business and Financial Sciences. With extensive academic and professional experience, Dr. Titi has taught courses in Cybersecurity, Cloud Computing, and Data Encryption, and supervised various student projects. His research interests include Cloud Computing, IoT, Network Security, and e-Learning. He has published several research papers and authored books in his fields of expertise. Dr. Titi is also certified in MCP, Network+, and A+, and has conducted workshops on e-learning and quality assurance.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.