An Analytical Study of Information Security Awareness in Palestinian Institutions in the West Bank

Tahany Kmail, Mousa M. Farajallah, Ibrahim R Al-Sharif

***Abstract* — This study examines the current level of information security awareness and assesses the effectiveness of training programs within Palestinian institutions. Although cybersecurity has become increasingly important, many individuals still lack formal training, which raises the risk of security breaches. To explore this issue, an online questionnaire was shared with employees and students across various organizations in Palestine. The survey focused on their behaviors, attitudes, and preferences regarding awareness efforts and training approaches. The results highlighted gaps in training quality, and participants preferred interactive methods such as simulations and educational games. Many also noted that clear incentives or defined penalties would encourage better adherence to security protocols. In light of these findings, the study recommends implementing ongoing and customized awareness programs that suit specific workplace environments. Such measures are key to strengthening security culture and minimizing risks linked to human error.**

I. INTRODUCTION

In light of the accelerating digital transformation, organizations worldwide — and especially in Palestine — have become increasingly dependent on digital systems for daily operations in education, financial services, and government functions. This reliance has intensified due to the COVID-19 pandemic, recent conflicts, and ongoing instability in the West Bank. Consequently, both institutions and individuals have turned heavily to sensitive digital platforms such as e-learning, online banking, and e-commerce, making information security one of the most critical challenges, particularly in resource-limited contexts like Palestine [1]. Cyber threats — including data breaches, intrusions, and service disruptions — continue to rise, putting additional pressure on already strained infrastructures. Despite the growing significance of information security, many Palestinian institutions suffer from limited awareness among employees and students. This gap increases vulnerability to human errors that could lead to severe security incidents. Prior studies emphasize that technical measures alone are insufficient; the human factor remains vital in securing digital assets [2]. Unsafe behaviors often result from inadequate training and a lack of continuous awareness efforts [3]. Furthermore, the success of security strategies hinges on integrating effective awareness programs that consider user behavior and motivations [4]. The challenges in Palestine are compounded by limited funding, weak infrastructure, and a shortage of technical expertise [5]. This study explores the current state of information security awareness in Palestinian institutions, focusing on the effectiveness of existing training programs and employees' willingness to adopt secure practices when proper incentives and sanctions are applied. It examines preferences for various awareness-raising approaches, such as interactive training and simulations, and offers practical recommendations to build a sustainable culture of security [6].

The research Questions and Scope in this study aim to address the following questions:

To what extent are individuals aware of information security concepts and practices?

How effective are the current training programs in improving this awareness?

What factors support or hinder individuals' compliance with information security policies?

What types of awareness methods and training approaches do individuals prefer to enhance understanding and promote actual adherence?

The scope of the study is limited to institutions in the West Bank, focusing specifically on employees and students within these organizations.

II. LITERATURE REVIEW

In today's digital age, information security awareness (ISA) is a vital component of cybersecurity, especially in regions facing technological, political, and regulatory challenges that increase vulnerability. In Palestine, ongoing conflict, scarce resources, and growing digital threats make the development of effective and culturally relevant ISA initiatives all the more urgent. Although international studies provide useful frameworks, many originate from contexts quite different from the Palestinian environment. This review highlights key research on ISA from human, organizational, and policy angles, and points to future research priorities that align with Palestine's specific needs.

A. Human and Organizational Dimensions of Information Security.

Although technical solutions are essential for cybersecurity, researchers increasingly emphasize the decisive role of human factors in shaping secure practices [7] point to the significance of workplace culture, employee engagement, and the broader sociocultural environment in determining the success of ISA programs. These dimensions are especially relevant in Palestine, where occupation and conflict add pressures that influence daily life and organizational behavior. [8] introduced a multidimensional model linking individual, organizational, and societal factors to security attitudes and behaviors, providing a valuable framework for understanding

978-9950-8599-0-6

how awareness translates into action. However, this model has not yet been fully applied in Palestinian settings.

B. The Role of Policy and Leadership in Driving Security Awareness.

Strong policies, supported by committed leadership, are vital for creating environments where information security can thrive [9]. Found that in Gaza's universities, institutions with clear security policies and active awareness programs achieved better information system outcomes. These findings align with global research that stresses the need for policy-backed awareness efforts that are continuously reinforced through training. Yet, scholars argue that in Palestine, policies often lack the regulatory backing or institutional consistency needed to maximize their [7].

C. Information Security Awareness Among Palestinian Youth and Students.

Recent studies on Palestinian youth and students show varied levels of digital security knowledge. Observed that while many students understood basic practices like using strong passwords, fewer recognized more complex risks such as phishing or data privacy issues [10]. Digital platforms—including social media and smartphones—have emerged as promising tools for delivering ISA [11] [12]. These platforms, when combined with sound educational strategies, can help bridge knowledge gaps and engage students in meaningful ways, including addressing gender-based disparities in awareness.

D. Cybersecurity Threats and Digital Rights Under Occupation.

Conflict and political instability introduce unique cybersecurity threats. Documented how Palestinian youth face increased exposure to risks such as digital surveillance, identity theft, and online harassment [13][14]. The psychological toll, including anxiety and self-censorship, highlights the need for tailored awareness initiatives that build digital resilience. Furthermore, 7amleh's reports on rising hate speech, AI-driven incitement, and content censorship underline the urgency of national strategies that combine awareness efforts with legal protections to defend digital rights in Palestine.

E. Gaps in Research and the Way Forward.

Despite an expanding body of work on ISA, significant gaps remain. There is a need for applied, context-sensitive studies that assess the real-world impact of awareness initiatives in Palestine. Few studies integrate technical, behavioral, and policy perspectives into cohesive models suited to the local context. Future research should prioritize designing localized ISA frameworks, evaluating the psychological impacts of digital threats, and developing strategies that combine awareness, technology, and legal reforms to safeguard Palestinian digital spaces .The 2024 report from 7amleh's annual campaign revealed an unprecedented escalation in online hate speech against Palestinians, with over 12 million documented instances. The report advocates for immediate legal reforms and technical measures to combat digital incitement and uphold Palestinian digital rights [15]. The literature on information security awareness (ISA) in local and developing contexts reveals several key gaps that call for deeper investigation. These include the absence of strong theoretical frameworks, few applied studies, limited focus on cultural and behavioral aspects, and a lack of evaluations on the effectiveness of current programs. Highlight the need for models that reflect institutional and contextual specificities, as most existing frameworks do not account for the realities of governmental institutions in developing nations[7]. Prior research has paid substantial attention to security policies, yet few studies assess the impact of awareness and training initiatives in educational settings in countries like Palestine [9]. Furthermore, there is no unified definition of ISA, creating inconsistencies across studies [16]. Most models fall short in linking causal variables to security behaviors, and research remains concentrated in Western contexts, with limited focus on culturally tailored studies for developing regions. In Palestine, studies rarely apply theoretical models in practice or explore the role of cultural and social factors in shaping awareness [17]. There is also insufficient evaluation of digital versus traditional awareness strategies, and little attention to how students translate knowledge from digital media into daily practice [11]. While existing work documents digital threats and rights violations, few studies assess the outcomes of awareness strategies or propose improvements suited to Palestinian society [15]. There is also a need for research on legal and technological policy development, the psychological effects of digital threats, and strategies for addressing hostile online content [13][14]. This study's significance lies in its local focus and reliance on empirical data from students and employees in Palestinian educational and governmental institutions. It integrates technical, behavioral, and organizational dimensions within a model that reflects the cultural and institutional characteristics of Palestinian society. The study further addresses gaps related to the effectiveness of training programs in contexts marked by technical, human, and political challenges, and explores how personal and organizational factors shape digital security behavior, offering insights that support the development of more effective, locally grounded policies and programs.

III. METHODOLOGY

This research is classified as a quantitative, descriptive, and analytical study. It was selected for its suitability to the study's objective: measuring the level of information security awareness among employees in Palestinian government institutions, identifying the key variables influencing this awareness, and examining their attitudes towards training methods and various awareness channels. The significance of this design lies in its ability to provide precise quantitative insights that reflect the current level of understanding of information security within the government work environment. It also enables comparative analysis across different categories, such as department or years of experience, to identify potential strengths and gaps in awareness across the organization. An electronic questionnaire was specifically developed for this purpose,

drawing on the components of information security awareness as outlined in academic literature and professional standards (such as NIST and ISO/IEC 27001). These components include: awareness of risks, security-related behaviors, responses to threats, and employee preferences regarding training programs. The following is Fig. 1, which illustrates the methodology followed.

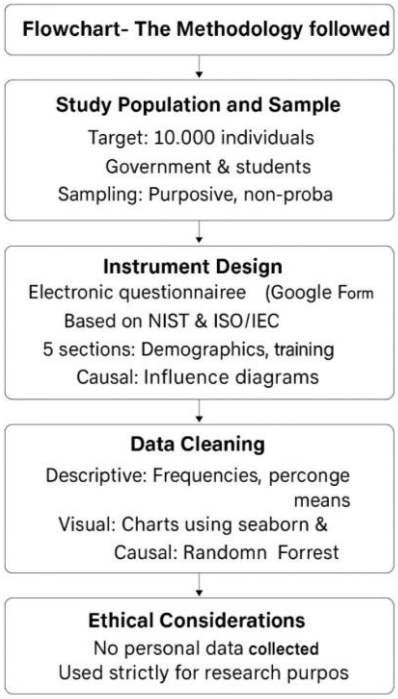


Figure 1 .The methodology followed.

A. Study Population and Sample.

The study population consisted of approximately 10,000 individuals, including government employees and students from various public institutions, distributed across administrative and technical sectors in the northern West Bank governorates. The target population included individuals who work directly or indirectly with digital systems, sensitive data, or internal networks, as they are considered the group most vulnerable to information security risks and cyber breaches. The final sample size was 8,200 respondents who successfully completed the online survey.

A non-probability purposive sampling method was used, where participants were deliberately selected based on the nature of their work in relevant departments, such as information technology support, information systems, general administration, human resources, finance, and education. The sample also included high school and university students. The study ensured that the sample was diverse in terms of gender, age group, and work experience, with the goal of providing a comprehensive and representative understanding of information security awareness levels across the target segments. It should be noted that the sample adopted a non-random, purposive sampling method and included employees and students from various government institutions, noting that students constituted the largest proportion of participants. Students were intentionally included as a key target group for information security awareness programs, especially given the significant expansion in the use of digital educational systems and electronic services in government institutions. Students' security awareness is also an important element in enhancing organizations' digital protection, given their constant interaction with government entities' technical infrastructure. Although the sample included employees from various sectors, the predominance of students may partially affect the generalizability of the results to all other job categories. Therefore, future studies are recommended to achieve a greater balance between the target groups by designing more representative samples using random methods whenever possible.

B. Data Collection Tool.

The online survey tool was developed using Google Forms. The structure of the tool is divided into five main sections, all of which focus on information security awareness, as shown in the following Table 1.

Table1 . Structure of the data collection tool.

Section	***Focus Area***	***Purpose***
1. General Information.	Gender, age group, department, and years of experience.	Analyze the impact of demographics on awareness.
2. Information Security Awareness and Training.	Type, frequency, effectiveness, preferred methods.	Assess training availability, quality, and preferences.
3. Security Attitudes and Behaviors.	Threat response, awareness importance, penalties/incentives.	Evaluate behaviors and motivation for secure practices.
4. Preferred Outreach Methods.	Preferred tools: email, posters, apps, games, etc.	Identify effective awareness communication channels.
5. Evaluation and Suggestions.	Evaluation of interest, improvement suggestions.	Gather feedback to improve awareness efforts.

The questionnaire was distributed via official email channels to government agencies and internal employee groups. It was shared electronically to align with the digital nature of work in most of these institutionsThe questionnaire began with an introductory section that included the following pointsA clear definition of the study's objectives (measuring awareness, identifying gaps, and improving training programs)An emphasis on the confidentiality of the data, ensuring that responses would not be linked to participants' identitiesA statement clarifying that participation was entirely voluntary and that participants could withdraw at any time without any consequences.

C. Data Analysis.

The Python programming language was used to perform data cleaning and analysis. Data cleaning involved removing null values and standardizing data formats. This cleaning is necessary to prevent confusion caused by missing or inconsistent values, thus improving the reliability of the results.

- Descriptive analysis: frequencies, percentages, means, and standard deviations were calculated for various

variables. This provides a basis for understanding the nature of the sample and helps in accurately interpreting the results.

- Visual Analysis: Illustrative graphics, including bar charts and heat maps, were generated to demonstrate relationships between variables. This enhances the ability to detect patterns and associations that may not be apparent from tables alone.
- Descriptive and visual analysis: A causal influence map (causal diagram) was used to analyze the relationships between variables and to identify potential pathways influencing employees' awareness of information security. This approach helped clarify causal relationships and enhance the understanding of key influencing factors within the studied context. This approach allows for understanding potential causal relationships and not just correlations, supporting deeper and more reliable conclusions about influencing factors.
- Quantitative analysis: The random forest model allows for the assessment of attribute importance, measuring the extent to which each independent variable impacts the prediction accuracy of the dependent variable by the contribution each attribute makes to improving the model's results. This analysis helped identify the factors most influential in employee awareness of information security. With these properties, the Random Forest model is a powerful tool for examining complex data and identifying key areas to focus on to enhance security awareness within organizations. It provides an objective way to identify key factors to focus on to improve security awareness.

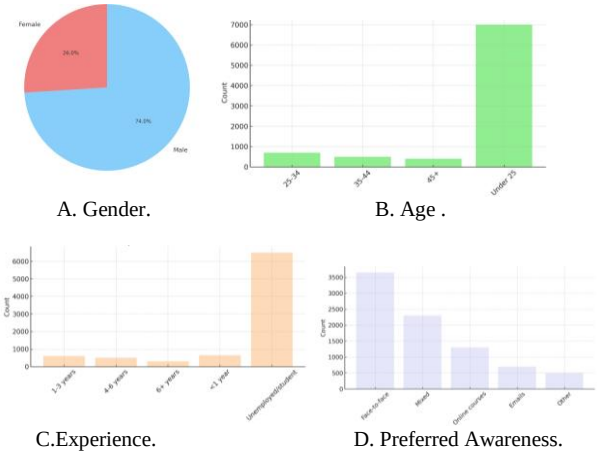
  In contrast, a regression analysis using the Random Forest algorithm showed that the "department" variable was the most influential factor on the level of security awareness, followed by "preferred awareness method," demonstrating the importance of functional dimensions and learning styles
- Inferential Analysis of Group Differences:In addition to the descriptive analysis, inferential analysis was conducted to verify the significance of differences between different groups in information security awareness. A one-way ANOVA was conducted to examine differences in "information security awareness" based on the "job department" variable. However, the results did not demonstrate statistical significance ($P > 0.05$). This indicates that the apparent disparity is not necessarily attributable to organizational differences. in shaping individual awareness. Other demographic variables, such as gender and age, had a relatively limited impact. Based on these findings, the study recommends developing awareness programs tailored to each functional department, providing diverse training content aligned with participants' media preferences (e.g., email, mobile apps, face-to-face meetings).

D. Ethical Considerations.

Ethical guidelines were strictly followed during data collection. The study's purpose was clearly explained in the questionnaire introduction. Participation was entirely voluntary, with no personal identifiers such as names or email addresses collected. The data was solely used for scientific research, and confidentiality was assured .Since the primary objective is to analyze and understand the influencing factors, the accuracy and validity of the data were carefully ensured through meticulous cleaning and comprehensive examination, along with the selection of appropriate statistical and analytical tools that ensure the reliability of the results and their reliance on sound and reliable data.

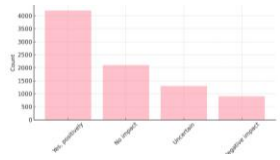
IV. RESULTS

In this section, descriptive results are presented regarding demographic factors and the level of security awareness and training among study participants. The data were analyzed and summarized using frequencies and percentages for various key variables to provide a clear picture of information security-related behaviors. The results showed that the majority of participants were male (74%), with the age group. Under 25 being the most represented (83%). Regarding departments, students accounted for 28%, followed by the finance department at 21%. In terms of work experience, 77% of participants were either unemployed or students. Concerning information security awareness, 82% indicated that they were unfamiliar with information security concepts, and 80% reported not receiving regular security training. Regarding reactions to suspicious messages, 47% preferred to delete the message immediately, while 29% chose to report it. Visual analysis was used to provide a deeper understanding of the relationships between the studied variables by generating several illustrative graphs using Python libraries such as Seaborn and Matplotlib. The graphs included: Bar charts: Used to display the distribution of responses across categories such as gender, age group, and educational level. These visualizations helped clearly illustrate the characteristics of the sample. It is shown in the following Fig.2

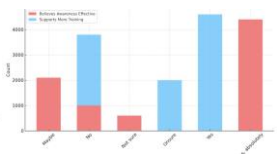


A. Gender. B. Age .

C.Experience. D. Preferred Awareness.



E. Training Usefulness.



F. Belief & Support.

A Causal influence map (causal diagram) was used to analyze the relationships between variables and to identify potential pathways influencing employees' awareness of information security. This approach helped clarify causal relationships and enhance the understanding of key influencing factors within the studied context. The causal influence map illustrates It is shown in the following Fig.3, the key factors that shape employees' knowledge of information security (Knows InfoSec) and their belief in the effectiveness of awareness efforts (Believes Awareness Effectiveness). The analysis reveals that prior experience plays a significant role in increasing the likelihood of receiving regular security training, which subsequently enhances employees' knowledge in the field. Additionally, demographic and organizational factors—such as gender, age group, and department—demonstrate a direct impact on information security knowledge. Notably, this knowledge acts as a mediating variable that influences how employees perceive the overall effectiveness of security awareness initiatives. These findings emphasize that enhancing information security knowledge requires not only structured and regular training but also an understanding of the underlying personal and institutional factors. Furthermore, strengthening this knowledge base positively contributes to cultivating employees' trust in the value of awareness programs.

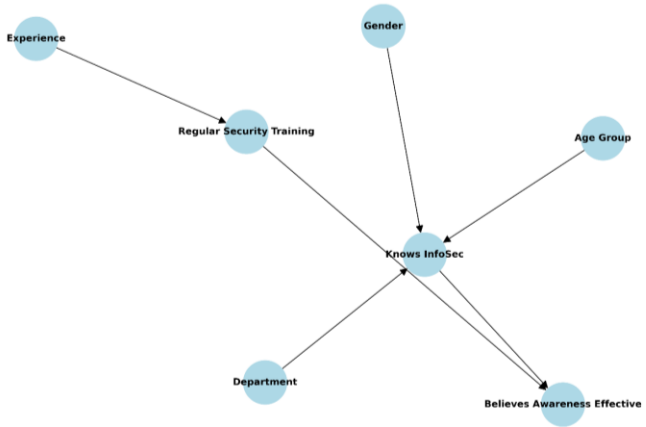


Figure 3 . Causal Effect Map.

In analyzing the factors influencing participants' awareness of information security, a feature importance estimation algorithm was employed to identify the most influential characteristics in the analytical modelthe results indicated that Department was the most influential variable, with an importance score of 0.118, followed by Preferred Awareness Method with a score of 0.103, and How Training Was Attended with a score of 0.087. These findings suggest that characteristics related to the nature of work and training play a fundamental role in shaping the level of security awareness. In contrast, demographic variables such as Gender and Age Group had a relatively smaller impact. This indicates that professional background and learning behaviors are more strongly associated with the level of security knowledge than personal factors. Fig. 4 visually illustrates the relative ranking of the variables, enhancing the understanding of the distribution of importance among the studied features.

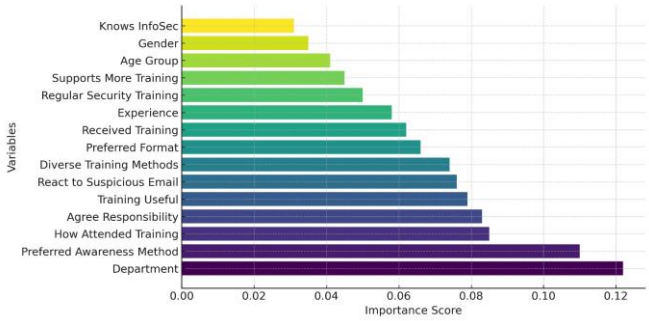


Figure 4. Visualization of Variable Importance in Security Awareness.

V. Discussion

The results of the analysis showed that a significant portion of Palestinian government employees have not received formal training in information security, indicating a clear gap in institutional-level security awareness programs[18]. This highlighted the lack of investment in cybersecurity in environments facing economic and political challenges, such as those found in parts of the Middle East.

Although some participants indicated that they had received previous training, their assessment of its effectiveness was low. This reflects the poor quality of the training provided and Possibly, the lack of modern, interactive approaches diminishes its practical impact on security behavior. This emphasized the effectiveness of active and interactive learning methods, such as simulations and educational games, in enhancing security awareness[19]. Moreover, the results revealed that participants were more likely to adhere to secure practices when incentives or the threat of penalties were present, underscoring the pivotal role of institutional policies in shaping cyber behavior. This finding supports the General Deterrence Theory [20], which suggests that the perception of sanctions and rewards influences compliance with information security policies. Regarding responses to suspicious emails, participants' behaviors varied, ranging from immediate deletion and reporting to, in some cases, opening attachments. This indicates inconsistency in the ability to make sound security decisions and underscores the need for ongoing, scenario-based training. This demonstrated that regular and targeted training improves employee behavior in response to real-world threats[21]. In terms of awareness delivery channels, participants expressed a preference for a diverse range of methods, including email, meetings, and mobile applications. This highlights the importance of

developing a multimedia awareness strategy that accommodates the varied preferences of
employees. Who stressed the importance of engaging staff through multiple channels to foster a cybersecurity-conscious culture[22]. Finally, the majority of participants expressed an interest in conducting regular assessments of cybersecurity awareness. While this is a positive indicator of internal recognition of cybersecurity's importance, it also points to the current absence of such evaluations in many organizations.

TABLE 2 SUMMARIZES THE MOST IMPORTANT RESULTS OF PREVIOUS STUDIES.

Comparison with Current Study Findings	***Key Insight***	***Implication***	***Supporting Study***
80% of participants reported they had never received formal InfoSec training.	Many employees lack formal InfoSec training.	Indicates institutional gaps in awareness programs.	[18]
Participants expressed low confidence in existing training programs and showed a preference for engaging alternatives.	Existing training is often perceived as ineffective.	Suggests the need for modern, interactive methods (e.g., simulations, games).	[19]
The survey revealed a stronger willingness to follow security policies when consequences were clear (incentives or penalties).	Employees are more likely to comply with reward or punishment systems.	Highlights the role of institutional policy and deterrence in shaping behavior.	[20]
Deleted suspicious emails, 29% reported them, others took no action — confirming behavioral variation.	Participants reacted differently to suspicious emails (some risky behavior).	Demonstrates varied cyber decision-making abilities; ongoing, scenario-based training is needed.	[21]
Participants preferred multiple formats for awareness, including mobile apps, email campaigns, and face-to-face sessions.	Most participants.	Emphasizes the need for multi-channel strategies that match user preferences.	[22]

Overall, these findings of this study confirm its ability to address the identified research gaps in the literature on information security awareness, particularly within the Palestinian context. By analyzing empirical data collected from employees and students in educational and governmental institutions, the study successfully overcame the limited local representation that characterized previous research focused on Western settings or theoretical models lacking practical application.

The analysis revealed that variables related to behavioral dimensions (such as a sense of responsibility and reactions to threats), organizational dimensions (such as functional department and diversity of training methods), and technical dimensions (such as prior knowledge of information security and evaluation of training effectiveness) played a prominent role in explaining levels of digital awareness and behavior.

The model of variable importance showed that the organizational dimension (Department) and the preferred awareness methods were the most influential, underscoring the need to design awareness programs that consider the local institutional and cultural context.

Thus, the study contributes to bridging the gap between theory and practice by presenting an explanatory model grounded in quantitative and field-based evidence, which can serve as a foundation for developing more effective, context-sensitive training policies.

VI. CONCLUSION

The study revealed that the level of information security awareness among employees in Palestinian government institutions remains below the desired standard. This shortfall is attributed to the lack of formal training, inconsistency in its delivery, and limited diversity in awareness methods. The findings also indicated a clear preference among employees for interactive approaches, such as simulations and educational games. Furthermore, employees responded positively to the implementation of incentives and penalties aimed at encouraging secure behavior. These results underscore the urgent need to invest in effective and innovative awareness programs to strengthen cybersecurity and data protection within government institutions.

Based on these findings, it is recommended In light of the findings, which revealed a general lack of awareness of information security and a lack of formal training among the vast majority of participants, the study recommends the development of interactive training programs based on simulations and realistic scenarios to enhance the ability of employees and students to respond to various security situations. The impact of functional divisions on awareness also underscores the importance of designing training content tailored to the nature of each department's work. On the other hand, the results showed participants' preference for a variety of awareness-raising methods, calling for a multi-channel strategy that includes email, smart apps, and face-to-face meetings. Additionally, the study indicated the effectiveness of incentives and penalties in enhancing compliance with security policies, so it is recommended that they be included in corporate policies to enhance compliance. Finally, given the high proportion of young and inexperienced participants, the study emphasizes the need to focus on basic security concepts in any future awareness program.

References

[1] A. AlHogail, "Design and validation of information security culture framework," Computers in Human Behavior, vol. 49, pp. 567–575, 2015.

[2] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: An action research study," MIS Quarterly, vol. 34, no. 4, pp. 757–778, 2010.

[3] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010.

[4] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear

that motivate protective security behaviors," MIS Quarterly, vol. 39, no. 4, pp. 837–864, 2015.

[5] E. Abu-Shanab, "Predicting trust in e-government: Two competing models," Electronic Government, an International Journal, vol. 15, no. 2, pp. 129–143, 2019.

[6] M. Siponen and A. Vance, "Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations," European Journal of Information Systems, vol. 23, no. 3, pp. 289–305, 2014.

[7] R. AlMindeel and J. T. Martins, "Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia," Information Technology & People, vol. 34, no. 2, pp. 770–788, 2021.

[8] L. Jaeger and A. Eckhardt, "When colleagues fail: Examining the role of information security awareness on extra-role security behaviors," Information & Computer Security, vol. 26, no. 2, pp. 206–220, 2018.

[9] A. S. Abdelwahed, A. Y. Mahmoud, and R. A. Bdair, "Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian universities in the Gaza Strip," International Journal of Information Science and Management (IJISM), vol. 15, no. 1, pp. 65–77, 2017.

[10] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of information security awareness among Palestinian learners," in Proc. Int. Conf. on Information Technology (ICIT), 2021, pp. 402–407.

[11] A. Al-Jawaldeh et al., "School-based nutrition programs in the eastern Mediterranean region: A systematic review," International Journal of Environmental Research and Public Health, vol. 20, no. 22, p. 7047, 2023.

[12] 7amleh, "2018 ،"مشاركٌ في ورشات الأمان الرقمي لمركز حملة. [Online]. Available: https://7amleh.org/post/1500-mshark-h-fy-wrshat-alaman-alrqmy-lmrkz-hmlh-fy-alaam-2018

[13] A. Mhajne, "The application of IHL on Israel's cyber strategies against the Palestinians," in Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions, 2024, pp. 152–170.

[14] 7amleh, "Palestinian digital rights during war – Hashtag Palestine 2023," 2023. [Online]. Available: https://7amleh.org/post/hashtag-palestine-2023-palestinian-digital-rights-during-war

[15] 7amleh, "Hashtag Palestine 2024 – Digital rights in wartime," 2024. [Online]. Available: https://7amleh.org/post/hashtag-palestine-2024-en

[16] E. Albrechtsen and J. Hovden, "Improving information security awareness and behavior through dialogue, participation and collective reflection: An intervention study," Computers & Security, vol. 29, no. 4, pp. 432–445, 2010.

[17] O. Albada and D. Eleyan, "Cybersecurity awareness of vulnerabilities: Attacks, solutions and cybersecurity behavior in Palestine: Literature review," Cybersecurity Journal, 2024. [Online]. Available

[18] S. Al-Janabi and I. Al-Shourbaji, "A study of cybersecurity awareness in the educational environment in the Middle East," Journal of Information & Knowledge Management, vol. 15, no. 1, p. 1650007, 2016.

[19] J. Abawajy, "User preference of cybersecurity awareness delivery methods," Behaviour & Information Technology, vol. 33, no. 3, pp. 237–248, 2014.

[20] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 31, no. 1, pp. 83–95, 2012.

[21] F. F. G. Alotaibi, "Evaluation and enhancement of public cyber security awareness," M.S. thesis, 2019. [Online]. Available

[22] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," Computers & Security, vol. 31, no. 8, pp. 983–988, 2012.