

Cyber security awareness strategies via Facebook An analytical study of the page of the Jordanian Anti-Cyber Crime Unit

استراتيجيات التوعية الأمنية السيبرانية عبر الفيسبوك
-دراسة لصفحة وحدة مكافحة الجريمة الالكترونية الأردنية-

Hiba CHAOUA
Mohammed El-Béchir El-Ibrahimi
University, Bordj Bou Arreridj- Algeria
hiba.chaoua@univ-bba.dz
Orcid : 0009-0008-2244-0126

Received: 31/03/2026 published: 11/06/2026
تاريخ النشر: 2026/06/11 تاريخ الاستلام: 2026/06/31

Article abstract:

This study aimed to identify cybersecurity awareness strategies deployed via social networks, specifically focusing on the official page of the Jordanian Cybercrime Unit. Adopting a descriptive survey research design, the study utilized a content analysis instrument to gather and analyze data from a purposive sample of 21 posts published during the year 2021. The empirical findings indicate that the platform relied on a broad-scale cybersecurity awareness strategy characterized by operational continuity, thematic and dissemination diversity, and a progressive increase in audience engagement. However, the communication strategy neglected continuous evaluation and failed to disclose information regarding campaign outcomes or cooperative efforts with social partner organizations, while exhibiting a primary reliance on an affective communication paradigm.

Key words : Strategies; cybersecurity awareness; Facebook; the page of the Jordanian Cybercrime Unit.

ملخص المقال :

هدفت الدراسة إلى التعرف على استراتيجيات التوعية الأمنية السيبرانية عبر الشبكات الاجتماعية بالتطبيق على صفحة وحدة مكافحة الجريمة الالكترونية الأردنية، اعتمد فيها على المنهج المسحي، باستخدام أداة تحليل المحتوى لتحليل وجمع البيانات من عينة قدرت بـ 21 منشورًا مما تم نشره خلال سنة 2021. ودلت النتائج على اعتماد الصفحة على استراتيجية توعية أمنية سيبرانية واسعة النطاق، اتسمت بالاستمرارية، والتنوع في الموضوعات وأساليب النشر، وتنامي حجم تفاعلية الجمهور معها، إلا أنها أغفلت جانب التقييم المستمر، وعدم تقديمها لمعلومات حول نتائج حملاتها، وجهود تعاونها مع المنظمات الاجتماعية الشريكة، إضافة إلى تركيزها على إستراتيجية اتصالية وجدانية بالدرجة الأولى.

كلمات مفتاحية: استراتيجيات؛ التوعية الأمنية السيبرانية؛ الفيسبوك؛ صفحة وحدة مكافحة الجريمة الالكترونية الأردنية.

Introduction

Today, we live in the age of information and the remarkable development of communication technology and digital information, along with its widespread use across all areas of life. This is due to the advantages offered by digital technology, such as the speed of communication and information exchange, as well as freedom from time and spatial constraints. We have thus become immersed in the virtual world through cyberspace. Statistics indicate that “the number of internet users worldwide increased from about 350 million in 2000 to approximately 3.366 billion by November 30, 2015, representing more than 46% of the world’s population, which exceeds 7.26 billion people” (Al-Dahshan, 2016, p. 86)

However, this rise in the number of users is accompanied by a decline in their level of training in how to use these technologies, which has increased their exposure to various risks—chief among them security threats. “A study conducted on a sample of students found that 33.3% had received threats via email, while 46.7% had been subjected to theft through the internet. Moreover, 60% indicated that their use of technology led to social isolation, and 46.7% reported acquiring inappropriate behaviors” (Al-Naghi & Mostafa, 2018)

This emphasizes the requirement for research into how to ensure the safe usage of cyberspace. The main official entities responsible for this are security/service agencies, which employ several methods/techniques, including social media.

This highlights the need to investigate the cybersecurity awareness strategies employed by solution/service organizations on social media. This is the focus of this study; our case study being the Facebook page of the Jordanian Cybercrime Unit. To conduct this study, a survey method was used with a content analysis instrument.

1. Study Topic

1.1 Research Problem:

Individuals interact within virtual communities often without being fully aware of the dimensions of this interaction or the security risks surrounding them. Security requirements are no longer limited to the physical society; in the age of technology, they have extended to the virtual world. Therefore, it has become essential for governments and both formal and informal organizations to consider and research methods and strategies capable of ensuring safety in cyberspace. Security institutions are among the most important official bodies tasked with maintaining public security and, specifically, cybersecurity, thereby contributing to national development and the creation of a safe digital society.

Perhaps one of the most important methods that security agencies can use for cybersecurity awareness is the use of modern communication tools such as social media networks. Communication through these platforms is characterized by three main features: scope, structure, and tone (Davis et al., 2014, p. 7)

The rapid rise of social media as a communication medium has allowed individuals to both consume and create information, thereby enabling informal and accessible two-way communication between law enforcement and the general public. Facebook is one of the many social media platforms that have created a need for security organizations to develop structured, clear cybersecurity awareness strategies in use of their site. These strategies must be methodical, well organized, and consistent with the credibility of the respective institutions while providing complete awareness programming. An example of such efforts is the Jordanian Cybercrime Unit Facebook page.

The research problem of this study is centered on attempting to uncover the cybersecurity awareness strategy adopted by the Jordanian Cybercrime Unit through its Facebook page. This is explored through the main research question: What are the cybersecurity awareness strategies employed via the Facebook page of the Jordanian Cybercrime Unit?

This main question gives rise to several sub-questions:

- What are the cybersecurity awareness strategies on the Facebook page of the Jordanian Cybercrime Unit in terms of topics?
- What are the cybersecurity awareness strategies on the Facebook page of the Jordanian Cybercrime Unit in terms of objectives?
- What are the cybersecurity awareness strategies on the Facebook page of the Jordanian Cybercrime Unit in terms of the level of interactivity?
- What are the cybersecurity awareness strategies on the Facebook page of the Jordanian Cybercrime Unit in terms of awareness methods?
- What are the cybersecurity awareness strategies on the Facebook page of the Jordanian Cybercrime Unit in terms of publishing tools?

1.2 Definition of Concepts:

This study addresses a set of terms that need to be clearly defined.

1.2.1 Social Media Networks:

Al-Maqdadi defines social media networks as: "A process of communicating with a number of people through websites and electronic services that enable the rapid dissemination of information on a wide scale. These platforms do not merely provide information; they interact and synchronize with users while delivering that information within their network. Thus, they represent a means of instant information exchange via the Internet" (Kamli, 2020, p. 610)

1.2.2 Facebook:

Facebook is considered one of the most popular social networking sites worldwide. "It was launched in February 2004 by Mark Zuckerberg at Harvard University in the United States as a platform for communication among students. The idea was later expanded to include employees and faculty members, and eventually anyone with an email address. Since then, Facebook has spread across different countries around the world, becoming one of the most widely used websites globally" (Shaishaa, 2020).

1.2.3 Cybercrime :

Refers to crimes committed against individuals or groups through contemporary telecommunication networks to deliberately destroy the individual's reputation or inflict direct or indirect physical, psychological, or other forms of damage . It impacts all sectors, including education, commerce, entertainment, and athletics. Cybercriminals, including hackers, partake in various illicit activities online, such as software piracy, virus deployment, bank fraud, online retail fraud, and numerous more offenses. (Hasan. Mehedi & all, 2025, p69)

1.2.4 Strategy:

A strategy is defined as setting long-term objectives, determining the appropriate means, allocating the necessary resources, and specifying the approach to dealing with opportunities and threats. Accordingly, a strategy has three main dimensions or elements: resources, plan, and goal.

Operationally, a strategy refers to a set of mechanisms and principles established by the security agency—in this study, the Jordanian Cybercrime Unit—using all necessary means, material resources, and human capacities through its page to achieve a strategic goal. This goal aims to reduce cybercrimes and raise users' awareness of the risks they face in their "second life" within virtual communities and cyberspace.

1.2.5 Security Awareness:

Security awareness is defined as the sensitivity and perception of anything that disrupts security or induces fear with the aim of achieving and consolidating security, whether it is moral or material, personal or familial, economic, political, military, or in other aspects of security (Badawi, 2020, p. 10).

Operationally, security awareness refers to the awareness-raising efforts carried out by the Facebook page of the Jordanian Cybercrime Unit to educate users about the various risks they face in virtual and cyberspace environments and how to avoid them.

1.2.6 Cybersecurity:

Cybersecurity is defined as the development of plans and the use of technical capabilities and tools to prevent unauthorized use and misuse, as well as to recover electronic information and the communication and information systems they contain... It also involves enhancing the protection, confidentiality, and privacy of personal data and taking all necessary measures to safeguard citizens and consumers from risks in cyberspace (Mousa, 2020, p. 550)

Operationally, cybersecurity refers to all measures and plans adopted by the security agency—the Jordanian Cybercrime Unit—to prevent any attempts at the unauthorized use of virtual and cyberspace environments that could cause harm to others' information.

1.2.7 Characteristics of Cybersecurity Awareness Frameworks:

Cybersecurity awareness frameworks are characterized by structured strategies and policies with continuous evaluation, comprehensive and integrated awareness, gradual and sustained dissemination, systematic and planned processes, and collaboration among diverse institutions (educational, media, political, religious, civil society, and governmental (Qashour & Sbeiti, 2021, p. 181)

1.2.8 Cybersecurity Patterns :

Cybersecurity domains constitute an integrated framework designed to protect digital assets across various technical and procedural dimensions. Based on authoritative references, the four requested domains are detailed as follows:

Network Security: Serving as the primary line of defense, it focuses on safeguarding network infrastructure and communication channels against both internal and external threats to maintain data integrity and confidentiality during transmission.

Information Security: This discipline encompasses the protection of data irrespective of its physical or digital state (including paper documents). It is conceptually broader than traditional cybersecurity, primarily governed by the principles of confidentiality, integrity, and availability.

Application Security: This domain involves fortifying software and applications against security vulnerabilities throughout their design and operational lifecycles, utilizing secure coding practices and regular patching.

Operational Security (OPSEC): Defined as a systematic risk management process, OPSEC aims to identify and protect sensitive information by analyzing organizational processes through the perspective of a potential adversary. This methodology is rooted in military strategic planning to ensure the secrecy of critical operations." (Al-Husseini, 2023, p62)

1.2.9 Principles of Cybersecurity Awareness Strategies:

For a cybersecurity awareness strategy to be effective and accepted in practice, it must follow the following fundamental principles:

Continuity: The strategy should be long-term and active over several years to ensure effectiveness and acceptance.

Clarity: Communication must be clear, simple, and easy to understand, free of contradictions, and the message should be comprehensible to the target audience.

Realism: Communication should reflect the truth about the content so that it is accepted by the audience; false information can distort the perception of the message.

Methodology and Organization: The foundations, objectives, and approaches of the strategy should be determined according to specific methods and programs.

Comprehensiveness: Cybersecurity awareness should cover all security-related fields and aim to reach all segments of society.

Integrate all stakeholders involved in security with an understanding of how each party is connected.

Innovate and Develop: Social development will require education to keep up with changes and adapt as the society changes.

Align with the Security Strategy: Cybersecurity awareness programming and objectives must align with the Security Strategy so that the overall goals will be achieved throughout all security domains (Noufel, 2018)

1.3 Previous Studies:

The research problem of this study is based on a number of previous studies, among which the following can be highlighted:

1.3.1 Study (Al-Dahla, 2018), titled: The Role of the Jordanian Cybercrime Unit's Facebook Page in Cybersecurity Awareness: An Analytical Study

This study aimed to examine the role of the Jordanian Cybercrime Unit's Facebook page in cybersecurity awareness. The researcher adopted the survey method using a content analysis tool to analyze posts published between January 1, 2017, and November 30, 2017, totaling 41 posts.

1.3.2 Study (Qashour Amal & Sbaiti Farah, 2021), titled: Awareness Strategies in the Social Media World Organized by the Lebanese Internal Security Forces

This study aimed to explore the concept of social media platforms and their impact on enhancing security, to examine the levels of Lebanese internal security, and to analyze cybersecurity awareness campaigns for social media users in the virtual world. It also investigated the dimensions of influence through guidance, regulation, and relevant laws and legislation, and finally addressed the obstacles in controlling the tools used.

1.3.3 Commentary on Previous Studies:

The current study aligns with previous research in its focus on studying cybersecurity awareness strategies across different topics on social media platforms. Our thorough examination will deal with the awareness of cyber security strategies and will do so distinctly from the Al-Dahli study which focused on awareness of cyber crimes as a component of cyber security.

2. Methodological Procedures of the Study

2.1 Type of Study and Methodology:

This research falls within descriptive studies, which focus on describing the nature, features, and characteristics of a specific phenomenon in order to gain insights about it

The study adopted an analytical survey method through both quantitative and qualitative analysis of a sample of posts from the Facebook page of the Jordanian Cybercrime Unit, using a content analysis tool.

2.2 Study Population and Sample:

"The study relies on the dimensions of topic and time to define the research population (Wimmer & Dominick, 2013, p. 287). In accordance with the primary research question, the population comprises all posts published on the official page of the Cybercrime Unit. The year 2021 was designated as the study's timeframe due to the high density of cybersecurity awareness posts, particularly those addressing cybercrimes. This period coincided with the COVID-19 pandemic and the implementation of quarantine and social distancing measures, which led to a sudden surge in cyberspace usage across various fields—often without prior preparation or awareness of the associated risks. A total of 111 cybersecurity awareness posts were identified from the page's overall content throughout the year.

A simple random sample was used, given the difficulty of identifying and tracking all members of the study population; this ensures equal opportunities for all units of the phenomenon under study. To ensure better representation, two posts were randomly selected from each month. This resulted in a sample of 21 units, reflecting a deficit of three units because the months of May, October, and December contained only one post related to cybersecurity awareness each

2.3 Data Collection Tool:

The study relied on the content analysis method, which in media studies requires defining categories within which the content of the study sample is analyzed, based on the research questions and the intended outcomes of the study.

2.3.1 Analysis Categories:

The study adopted content analysis as its primary tool, the analysis was based on a set of categories divided into three main axes:

- **Primary Data of the Sample:** This category was used to define the sample and describe all its elements.
- **“What Was Said” Categories (Content Categories):** These included the topic category, the objectives category, and the page interaction level category.
- **“How It Was Said” Categories (Form Categories):** This axis relied on a single category, which included the types of awareness methods and the multimedia tools used.

2.3.2 Units of Analysis:

The analysis relied on two units: the publication material unit and the idea unit. “Their presence or absence, and their frequency, provide the researcher with indicators useful for interpreting quantitative results” (Abdel Hamid, 2010, p. 135)

3. Presentation and Analysis of Study Results

After collecting and processing the data related to the study sample and its data collection tool, the following results were obtained:

3.1 Primary Data of the Sample:

One of the main features of Facebook is that when a user joins the site, they must create a personal profile containing the individual's personal information. The following table presents the key information provided by the official Facebook page of the Jordanian Cybercrime Unit.

Table 1: Sample Characteristics

Page Name: Jordanian Cybercrime Unit / **General Information:**

Information	Details
Description	Jordanian government organization
Date of Establishment	December 7, 2014
Website Link	http://www.psd.gov.jo/
Contact Information	Phone: +962 6 5633404, Email: ecrimes@psd.gov.jo
Location / Address	Amman, Jordan, 00962
Number of Page Likes	511k
Number of Followers	15

3.2 “What Was Said” Categories:

3.2.1 Topic Category:

The topic category is one of the most important categories in analyzing a communication message, as it helps identify the areas of focus of the communicator. In this study, this category was used to identify the different types of cybersecurity awareness topics covered by the Jordanian Cybercrime Unit’s Facebook page. The subcategories are presented in the following table:

Table 2: Types of Cybersecurity Awareness Topics in the Sample

Categories	Frequency	Percentage
Emerging Cybercrimes	6	18.18%
Committed Cybercrimes	4	12.12%
Initiatives and Programs	9	27.27%
Instructions and Guidelines	14	42.42%
Total	33	100%

The table shows that the most emphasized topics on the page were Instructions and Guidelines at 42.42%. These consist of information and regulations directed to the public on how to use the Internet correctly and safely.

The second most frequent topic covered in “Programs/Initiatives” (27.27%) included campaigns to raise awareness, media programs, and security initiatives related to investigations and arrests but did not report their outcomes. Emerging Cyber Crimes, at 18.18% of submissions, identify new and evolving threats such as cyber fraud and internet-based payment crimes. Finally, committed Cyber Crimes are reported at 12.12% indicating already documented crimes. Overall, there were several areas related to cyber crime that were not addressed in the previously mentioned categories including technology related acts of terrorism (Noufel, 2018, p. 264)

- Unauthorized access to information, such as stealing, deleting, or modifying it.
- Accessing server devices that provide information and sabotaging or disabling them.
- Obtaining information to change website addresses for the purpose of blackmailing public institutions.
- Illegitimate gain through exploiting information technology, such as credit card forgery and website hacking.
- Using technology to support terrorism and extremist ideologies.
- Identity theft for material gain.
- Extortion, threats, and defamation.
- Fraud and deception, such as selling fictitious goods or services.

3.2.2 Category: Objectives

This category refers to the awareness-related purposes that the unit aims to achieve among users through the page’s posts. They are divided as follows:

Table 03: Nature of Cybersecurity Awareness Objectives in the Sample

Categories	Frequency	Percentage
Protection and Prevention	15	28.30%
Interaction and Trust Building	7	13.20%
Activation of Collaborative Relations	7	13.20%
Information and Guidance	19	35.84%
Deterrence and Scaring Off Criminals	5	9.43%
Total	53	100%

The table data indicates that, based on our analysis of the Cybercrime Unit's Facebook page, the unit primarily aims to educate and guide by identifying and detailing various cybercrime methods and issuing warnings regarding them, in addition to providing information, advice, and guidance on the safe use of cyberspace, with this category accounting for the highest percentage at 35.84%.

The Cybercrime Unit also seeks, through its page, to achieve **“protection and prevention,”** which ranked second at 28.30%. This objective concerns efforts to protect users from all types of cyber risks, including legal protection, protection against financial fraud in cyberspace, and protection from breaches and theft of private data.

Meanwhile, the objectives related to **“interaction and trust building”** and **“activation of collaborative relations”** came in third place, with equal percentages of 13.20% each. As Al-Najjar (2010, p. 35) notes, *“the police in any society constitute a human and social system that both influences and is influenced by the multiple forces within that society.”*

While the goal of **“intimidation and deterrence”** came last with a small percentage estimated at 9.43%, where the unit sought through its page to intimidate internet users of legal procedures and penalties resulting from committing cybercrimes.

3.2.3 Interactivity Category

One researcher defined interactivity as one of the most important features of the information society. It refers to the ability of the communication receiver to engage with other participants and continuously exchange feedback on information and network components based on the responses they observe. Interactivity is characterized by networking, meaning complete linkage (Khafaga, 2020, p. 193)

In this study, the interactivity category allows for determining the degree of audience engagement with the page through the various types of interactions that Facebook pages provide for published topics. It enables the audience to express their opinions and attitudes toward the content, such as likes, comments, and shares, where clicking on any of these contributes to the spread of the post and its delivery to other users, particularly through sharing.

Table 04: Interaction Volume by Number and Type of Interactions

Average Number of Interactions per Post	Percentage	Frequency	Categories
786.76	81.06%	16,522	Like
121.66	12.83%	2,555	Comment
62.04	6.39%	1,303	Share
—	100%	20,380	Total

High amounts of engagement over different kinds of ways to interact will help the content on the page reach more and more users through social media channels. The average amount of each of the types of interaction is also much higher than what would typically be seen as there is an average of 786.76 likes, 121.66 comments, and 62.04 shares per post respectively. This indicates that audiences are engaged at a much higher level than what was experienced with the posts used in this sample.

This result contrasts with the findings of a previous study by Mohamed Hisham Al-Dahla, who reported limited audience engagement with the Facebook page of the Jordanian Cybercrime Unit. In his study, the **“low” category (0–250 likes)** recorded the highest percentage of likes at 38.88%, the **“low” category (0–35 comments)** recorded the highest percentage of comments at 46.27%, and the **“low” category (0–15 shares)** recorded the highest percentage of shares at 72.18% (Al-Dahla, 2018, pp. 74 -75)

The page's early limited reach is linked to its recent creation and low internet use before COVID-19, while the pandemic increased digital reliance and engagement. Despite improved reach and continuity, interaction remains mostly passive, dominated by likes (81.06%) with fewer comments and shares, suggesting limited

audience participation and highlighting the need to encourage more active engagement and content sharing (Al-Dahla, 2018, p. 74).

3.3 “How It Was Said” Categories

3.3.1 Methods Category

It is well known that several communication strategies are employed when publishing media content through social media. These strategies depend on the nature of the message’s objective and the intended audience. They can be summarized as follows:

- **Cognitive Strategy:** Aims to provide the audience with informational and descriptive data.
- **Affective (Emotional) Strategy:** Aims to influence the audience’s emotions and sentiments.
- **Behavioral Strategy:** Aims to guide the target audience to perform specific behaviors (Meziane, 2021, p. 1026)

Through this category, we aim to identify the range of methods used by the page administration to raise awareness among Internet users, in order to achieve cybersecurity for the Kingdom and its citizens, and thereby determine the type of communication strategy adopted by the page.

The methods category has been divided into the following subcategories:

- **Guidance and Direction:** Refers to the instructions and guidance provided by the page to enable users to navigate the Internet and to use certain websites and programs correctly.
- **Warning and Awareness:** Refers to the information through which the page alerts users to potential risks to prevent them from falling victim to cybercrime.
- **Legal Information:** Refers to all information about cybercrime laws provided by the page to inform and educate users.
- **Information on Deterrent Punitive Measures:** Refers to all content posted on the page concerning legal sanctions against those who commit offenses related to cybercrime law.
- **Usage Systems:** Refers to information provided to the audience on how to correctly use certain websites and programs on the Internet.
- **Reporting Awareness Activities:** Includes all media activities and initiatives conducted by the unit and published on the page.

Table 05: Types of Cybersecurity Awareness Methods in the Sample

Categories	Frequency	Percentage
Guidance and Direction	6	18.75%
Warning and Awareness	8	25%
Legal Information	4	12.5%
Information on Deterrent Punitive Measures	4	12.5%
Systems and Methods of Secure Use	3	9.37%
Awareness Media Campaigns	7	21.87%
Total	32	100%

An analysis of the study sample underscores the multiplicity of awareness-raising methodologies deployed by the Unit. Furthermore, a quantitative assessment of the percentage distribution demonstrates that

the Cybercrime Unit's platform relies most heavily on warning and threat-sensitization techniques regarding the risks of cyber-victimization, which constitute 25% of the total output. This is followed by informational reporting on the Unit's awareness initiatives at 21.87%, and instructional and guidance protocols at 18.75%. In contrast, methods designed to introduce cybercrime legislation and those detailing deterrent punitive mechanisms both occupied the fourth position, representing a modest 12.5% each. Lastly, the dissemination of information regarding safe usage systems comprised the smallest share at 9.37%. Based on the empirical data pertaining to these classifications, it is highly evident that the Cybercrime Unit has predominantly executed an affective communication strategy, followed sequentially by cognitive and behavioral strategies

3.3.2 Multimedia Category

Multimedia simply refers to more than one medium, meaning the use of a combination of text, images, sound, and motion.

This category includes the types of multimedia used in posts on the page, as shown in the following table.

Table 06: Types of Publishing Media Used in Cybersecurity Awareness in the Sample

Categories	Frequency	Percentage
Text	1	4.76%
Image	1	4.76%
Animation	1	4.76%
Text + Graphics	12	57.14%
Text + Image	4	19.04%
Text + Video	2	9.52%
Total	21	100%

The table data show the page's strong reliance on multiple media in a single post, with the majority of posts combining text with graphics—whether diagrams, infographics, or illustrative drawings—at 57.14%. This is followed by text with image at 19.04%, then text with video at 9.52%, while text alone and image alone were least used, each at 4.76%.

It is worth noting that all texts in the sample posts included hyperlinked text at the end in the form of hashtags, which are among the most widely used links on social media platforms. Clicking a hashtag directs users to all content related to that topic, a technique that increases the effectiveness of interactions on the page and helps expand the reach of posts.

Finally, it is worth noting that the page neglected the use of audio as a medium.

4. General Results of the Study

The study results demonstrate that the Unit deployed a broad-scale and sustained awareness strategy; however, it was fundamentally anchored in an affective communication paradigm. This model focused on the risks and threats associated with technological usage by leveraging emotional arousal—specifically the fear of punishment, scandal, and extortion—while stimulating the desire for security, rather than providing cognitive-procedural explanations regarding the underlying structure of technical threats. In this regard, psychological and behavioral literature indicates that emotional arousal serves as a potent mechanism for capturing attention and eliciting immediate, reflexive responses from the target audience. Recently, the affective dimension of communication has become increasingly salient within a volatile information ecosystem plagued by misinformation and disinformation, where the efficacy of logic and rationality diminishes as emotional engagement intensifies. Cognition often follows suit with our feelings, thus presenting the risk of emotional fallacy (Andre, 2025, p9). Consequently, an over-reliance on warning-centric messaging—absent clear cognitive empowerment—may trigger adverse reactions, as users may resort to

avoiding awareness-related content as a defense mechanism to mitigate anxiety levels (Bhattacharjee & Singha, 2026, p. 2). this finding is substantiated by the following indicators :

4.1. Cybersecurity Awareness Strategies Adopted by the Page: Thematic Content

The results regarding the "thematic category" revealed a diversity of topics, alongside a clear commitment to various activities, initiatives, and awareness campaigns. Furthermore, the page featured security-related activities such as criminal investigation, crime tracking, and offender apprehension. However, a significant critique of this strategy is the omission of continuous evaluation for these programs and campaigns. The failure to provide data on outcomes and impacts may undermine the audience's trust in the page. This is reflected in several negative user comments, such as: "Providing advice is very useful, but providing the service is better... I filed a complaint nine months ago, and no action has been taken yet." This aligns with Sergeant's (Harriet, 2018, p8) assertion that "the test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with them". Additionally, the scope of these topics' lacks comprehensiveness regarding various cybersecurity and electronic crime issues, as it neglects the use of technology in supporting terrorism—a critical issue in our contemporary society, as previously mentioned.

4.2 .Cybersecurity Awareness Strategies Adopted by the Page: Objectives

The page's primary objective is to educate and guide by identifying and detailing various cybercrime methods while issuing warnings against them. This is in addition to providing a range of information, advice, and guidelines on the safe use of cyberspace, as education is considered the first step and a fundamental goal in overcoming the greatest barrier to awareness: ignorance.

Furthermore, the Cybercrime Unit aims through its page to achieve 'protection and prevention', which ranked second. Protection and prevention constitute a fundamental requirement and a long-term output of cybersecurity awareness programs and operations. This outcome reflects the page's reliance on structured and goal-oriented execution, since fostering security awareness requires sequential stages that 'commence with the dissemination of knowledge to correct erroneous information, proceed to modifying undesirable attitudes, and ultimately culminate in behavioral change' (Nofal, 2018, p. 266), thereby establishing secure awareness and behavior. Nonetheless, the page is criticized for disproportionately focusing its guidance on highlighting risks and threats .

However, focusing on the risks may have counterproductive effects on the target audience's psychological state.

Conversely, the study revealed that the page does not emphasize deterrence or the intimidation of criminals. This aligns with the intrinsic nature of the medium, as social media platforms are characterized by their reliance on an informal tone when engaging with the public. This finding is highly consistent with the principle of voluntary prevention embedded within security awareness strategies.

This result also aligns with the principle of voluntary prevention within security awareness strategies. Objectives related to "interaction and trust-building" and "fostering collaborative relationships" ranked third, aiming to achieve cooperation between security and community institutions. However, the page is criticized for overlooking collaboration with primary socialization institutions (namely, the school and the family).

.4.3Cybersecurity Awareness Strategies Adopted by the Page: Interactivity Levels

Continuity is a cornerstone of any effective strategy. The study demonstrated the page's success in terms of reach, continuity, and the increasing volume of audience interaction (likes, comments, and shares). However, despite high engagement levels, the study found that "Likes" were the predominant form of interaction. This reflects a limitation in the depth of engagement, which may restrict the algorithmic reach of posts and hinder information from reaching the widest possible audience.

.4.4Cybersecurity Awareness Strategies Adopted by the Page: Awareness Methods

The platform relies predominantly on warning and threat-sensitization techniques regarding the risks of cyber-victimization , followed sequentially by informational reporting on awareness-raising initiatives, and subsequently, instructional guidance. This pattern indicates that the Cybercrime Unit, through its digital presence, has executed a primarily affective communication strategy , followed sequentially by cognitive and behavioral paradigms. This communication model may ultimately have an adverse bearing on the nature of

the impact generated among the recipient audience, limiting it to a transient, emotional response that lacks long-term durability and sustainability.

4.5 Cybersecurity Awareness Strategies Adopted by the Page: Publication and Awareness Media

The results of the analysis highlighted the page's strong reliance in its posts on the multiplicity and diversity of means in a single post. This is a positive indicator of the page's effort to enhance clarity and ensure the target audience achieves the desired level of comprehension and perception.

The results of the analysis highlighted the page's strong reliance in its posts on the multiplicity and diversity of means in a single pos

Conclusion:

According to the results of the Cybercrime Unit's analysis, the Unit created an impressive, well-organized strategy to raise public awareness of cyber security threats and promote cyber safety. The Cybercrime Unit achieved a high level of visibility and participation through its Cyber Safety Facebook page, due primarily to the education, guidance and collaboration they focused on with their campaigns. However, there were many identified weaknesses that the Unit needed to address; such as lack of ongoing assessment of their campaigns and their outcomes, as this could hinder public confidence in the Unit. The Unit also did not cover or promote enough of the various types of cyber security threats and risks that were relevant to the Facebook audience. Additionally, the Unit relied heavily on appealing to the emotions of the viewer rather than creating behavioural changes over the long term. Finally, the Cybercrime Unit should be working towards developing partnerships and collaborative efforts with community-based organizations, schools, and families in order to create a stronger framework for creating an effective cyber safety awareness campaign.

Sources and references

- Abdel Hamid, M. (2010). *Content Analysis in Media Research*. Alam Al-Kutub.
- Al-Dahla. (2018). *The Role of the Cybercrime Unit Facebook Page in Security Awareness: An Analytical Study*
- Al-Dahshan, J. A. (2016). Digital Citizenship as an Approach to Arab Education in the Digital Age. In *Naqd wa Tanweer [Critique and Enlightenment]*, 2(5), 71–104.
- Al-Naghi, W. M. M., & Mostafa, H. M. H. (2018). The Effectiveness of a Program for Developing Digital Citizenship Values among Preparatory Stage Students in Light of Media Education. In *Journal of Media Research*(50), 601–642.
- Badawi, A. A. A. (2020). Requirements for Developing Security Awareness among Saudi University Students. In *The Comprehensive Multidisciplinary Electronic Journal for Publishing Scientific and Educational Research*(31), 1–34.
- Davis, E. F., Alves, A. A., & Sklansky, D. A. (2014). Social media and police leadership: Lessons from Boston. *Australasian policing*, 6(1), 10-16.
- Kamli, R. (2020). Social Media and the New Impetus of Globalization: The Impact of Social Media in the Arab World in Light of Globalization. In *Algerian Journal of Social and Human Sciences*, 8(2), 601–620.
- Khafaga, A. M. (2020). Communication and Interaction Tools on Social Networks as a Product and a Process: An Analytical Study on News Pages during Major Events. In *King Abdulaziz University Journal*, 28(9).
- Meziane, A. (2021). Persuasion Strategies in Health Messages on Social Media: An Analytical Study of Several Facebook Pages. In *Al-Mi'yar Journal*(53).
- Mousa, H. H. (2020). The Strategic Vision of Iraqi National Security in Cyberspace: An Approach between the Security Dilemma and Performance Capability. In *Algerian Journal of Legal and Political Sciences*, 57(5).
- Noufel, A. M. F. (2018). Security Awareness among a Sample of Police Officers' Children. In *Scientific Journal of the Faculty of Kindergarten*, 4(4).
- Qashour, A., & Sbeiti, F. (2021). Awareness Strategies in the World of Social Networks—Organized by the Directorate of Lebanese Internal Security Forces. In *Research Papers Journal*, 1(1).



- Shaishaa, A. (2020). *The Role of Social Networking Sites in the Political Communication Process: The Egyptian Case as a Model*. <https://www.academia.edu/11777389>
- Weimr, R., & Dominic, J. (2013). *Introduction to Media Research Methods* Translated by Saleh Abu Asba' & Mansour Farouk. Beirut: Center for Arab Unity Studies.
- Hasan.M, Sampa.M & Mahmud.M.K . (2025). «Understanding Cybersecurity Awareness Among Students in Bangladesh: A Data-Driven Approach», *Society& Sustainability*, 7(1), p 67-76.
- Harriet, t. (2018). *The Public and the Police Civitas*. First published .London. Institute for the Study of Civil Society The Cromwell Press .
- Andre ,V. (2025), *AN EMOTIONALLY BASED STRATEGIC COMMUNICATION APPROACH TO NATO PUBLIC SUPPORT IN BOSNIA AND HERZEGOVINA*, Publisher Atlantic Initiative, p9, <https://atlanticinitiative.org/wp-content/uploads/2025/02/Policy-Paper-An-Emotionally-Based-Strategic-Communication-Approach-to-NATO-Public-2025-ENG.pdf>
- Bhattacharjee ,S & Singha, S, S. (2026), *Revisiting Human-Centric Cybersecurity: The Influence of Online Cognition on Security Behaviour Intention*, *International Journal for Multidisciplinary Research (IJFMR)*, 8 (2), p1-6.
- Al-Husseini, F. A. (2023). *Cyber security awareness: luxury or necessity in the age of informaties*. *Journal of Research and Education*, 13(2), 54–74.