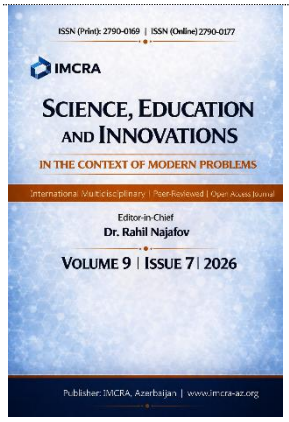

Science, Education and Innovations in the Context of Modern Problems
Issue 7, Vol. 9, 2026

RESEARCH ARTICLE

Cybersecurity Awareness and Its Role in Addressing Cyber Threats in the Digital Media Environment: A Survey Study of Digital Media Journalists in Algeria

Nassima Lounis

Faculty of Information and Communication Sciences University of Algiers 3
Algeria
E-mail: nassima.lounis@yahoo.fr

Keywords cybersecurity awareness; cyber threats; digital journalism; digital media; journalists; information security.

Abstract

The rapid digital transformation of contemporary journalism has fundamentally reshaped news production, distribution, and audience engagement while simultaneously exposing media professionals to an increasingly complex spectrum of cyber threats. Journalists working in digital media environments have become frequent targets of cyberattacks, including phishing campaigns, account compromise, ransomware, surveillance, identity theft, and unauthorized access to confidential information. Within this context, cybersecurity awareness has emerged as a critical professional competency for safeguarding journalistic integrity, protecting confidential sources, and ensuring the resilience of digital news organizations. This study investigates the role of cybersecurity awareness in mitigating cyber threats among digital media journalists in Algeria. Employing a descriptive survey design, data were collected through an online questionnaire administered to a purposive sample of 50 digital media journalists. The study examines journalists' understanding of cybersecurity concepts, their awareness of cyber risks, their adoption of secure digital practices, and their perceptions of cybersecurity awareness as a mechanism for strengthening resilience against cyber threats. The findings indicate that respondents demonstrate a relatively high level of cybersecurity awareness and possess a clear understanding of the evolving cyber risks associated with digital journalism. Participants recognized cybersecurity as an essential component of professional journalistic practice and reported adopting a range of protective measures to enhance digital security. The results further reveal that cybersecurity awareness significantly contributes to improving journalists' ability to identify, prevent, and respond to cyber threats while protecting media content, confidential information, and communication channels. The study concludes that strengthening cybersecurity awareness should be regarded as a strategic priority for media organizations, educational institutions, and policymakers. Continuous cybersecurity education and professional capacity-building programs are essential for enhancing journalists' digital resilience, protecting press freedom, maintaining information integrity, and reinforcing public trust in digital media within an increasingly hostile cyber environment.

Citation

Lounis, N. (2026). Cybersecurity Awareness and Its Role in Addressing Cyber Threats in the Digital Media Environment: A Survey Study of Digital Media Journalists in Algeria. *Science, Education and Innovations in the Context of Modern Problems, 9*(7), 1–16.
https://doi.org/10.56334/sei/9.7.21

Received: January 10, 2026 **Accepted**: May 09, 2026 **Published Online**: July 20, 2026

Introduction

The digital transformation of the global media landscape has profoundly redefined the ways in which information is produced, disseminated, and consumed. Advances in internet technologies, mobile communication, cloud computing, and social media

platforms have accelerated the transition from traditional forms of journalism to highly interactive digital media ecosystems. Digital journalism has consequently become one of the principal channels through which societies exchange information, shape public opinion, influence political decision-making, and facilitate social and cultural interaction.

While digital transformation has substantially enhanced the speed, accessibility, and interactivity of media communication, it has simultaneously expanded the cyber threat landscape confronting journalists and media organizations. Contemporary journalists increasingly rely on digital technologies for news gathering, source communication, data storage, collaborative reporting, and audience engagement. This dependence has made them attractive targets for a wide range of cyberattacks, including phishing, malware infections, ransomware, credential theft, social engineering, surveillance, distributed denial-of-service (DDoS) attacks, and unauthorized access to confidential information.

Cyberattacks targeting journalists extend beyond technical disruptions. They threaten editorial independence, compromise the confidentiality of information sources, undermine investigative journalism, and ultimately erode public confidence in media institutions. The protection of digital identities, communication channels, and sensitive journalistic information has therefore become an essential prerequisite for ensuring the continuity, credibility, and ethical integrity of modern journalism.

Algeria has experienced significant digital transformation within its media sector over the past decade. The rapid expansion of online news platforms, digital broadcasting services, and social networking applications has fundamentally altered journalistic practice and public access to information. As digital journalism continues to expand, Algerian journalists increasingly encounter cybersecurity challenges associated with their professional activities. These challenges expose media professionals to cyber risks capable of compromising sensitive information, disrupting journalistic operations, and threatening both personal and organizational security.

Within this evolving environment, cybersecurity should no longer be regarded solely as a technical concern reserved for information technology specialists. Rather, it constitutes an interdisciplinary professional competency encompassing technical knowledge, risk awareness, ethical responsibility, and secure digital behavior. Effective cybersecurity practices enable journalists to protect confidential sources, preserve data integrity, secure communications, defend digital identities, and maintain the authenticity of published information. Consequently, cybersecurity awareness represents a fundamental component of responsible digital journalism and an indispensable element of professional media practice.

Growing international concern regarding cyberattacks against journalists has highlighted the importance of strengthening cybersecurity literacy across the media sector. Journalists who possess higher levels of cybersecurity awareness are more capable of recognizing emerging cyber risks, implementing preventive security measures, responding effectively to cyber incidents, and reducing vulnerabilities associated with digital reporting. Conversely, insufficient cybersecurity awareness may expose journalists and media organizations to severe operational, legal, ethical, and reputational consequences.

Despite increasing global attention to cybersecurity in journalism, empirical evidence concerning cybersecurity awareness among journalists in developing digital media environments remains relatively limited. In Algeria, existing research addressing cybersecurity from the perspective of professional journalists remains particularly scarce. This knowledge gap underscores the need for empirical investigations examining journalists' awareness of cyber threats, their cybersecurity practices, and the role of cybersecurity awareness in strengthening digital resilience within the media sector.

Against this background, the present study investigates the contribution of cybersecurity awareness to addressing cyber threats among digital media journalists in Algeria. Specifically, the study explores journalists' understanding of cybersecurity concepts, evaluates their awareness of cyber risks associated with digital journalism, examines the cybersecurity practices they employ in their professional activities, and assesses how cybersecurity awareness enhances their capacity to prevent and mitigate cyber threats.

Accordingly, the study seeks to answer the following principal research question:

What role does cybersecurity awareness play in addressing cyber threats among digital media journalists in Algeria?

To address this question, the study examines the following research questions:

1. What is the level of cybersecurity awareness among digital media journalists in Algeria regarding the concept, objectives, and significance of cybersecurity?

2. To what extent are digital media journalists aware of the cyber threats and vulnerabilities associated with digital journalism?

3. Which cybersecurity practices are adopted by journalists to protect digital identities, confidential information, communication channels, and journalistic sources?

4. How does cybersecurity awareness contribute to strengthening journalists' capacity to prevent, detect, and respond to cyber threats within the digital media environment?

2. Literature Review

2.1. Cybersecurity Awareness in Digital Journalism

The rapid digitalization of journalism has fundamentally transformed the media ecosystem, creating unprecedented opportunities for information dissemination while simultaneously exposing journalists to increasingly sophisticated cyber threats. Contemporary journalists rely extensively on digital technologies, cloud-based platforms, social media, encrypted communication tools, and mobile devices for news gathering, verification, production, and distribution. Although these technologies have enhanced journalistic efficiency and audience engagement, they have also expanded the attack surface available to cybercriminals, making journalists attractive targets for cyberattacks (International Telecommunication Union [ITU], 2023; Kaspersky, 2024).

Cybersecurity awareness refers to an individual's understanding of cyber risks, knowledge of information security principles, and ability to adopt appropriate behaviors that minimize digital vulnerabilities. Within journalism, cybersecurity awareness extends beyond technical competence and encompasses ethical responsibility, protection of confidential sources, preservation of information integrity, and secure communication practices. Journalists with higher levels of cybersecurity awareness are generally better equipped to recognize malicious activities, implement preventive security measures, and respond effectively to cyber incidents before they compromise sensitive information.

Recent studies have emphasized that cybersecurity awareness is closely associated with secure online behavior. Garcia and Bongo (2022) found that individuals possessing greater cybersecurity knowledge demonstrated significantly better security practices, including stronger password management, safer online communication, and increased awareness of phishing attacks. Similarly, OPSWAT (2023) highlighted that basic cybersecurity behaviors—such as the use of complex passwords, password managers, and multi-factor authentication—substantially reduce the likelihood of unauthorized access to digital accounts.

2.2. Cyber Threats in the Digital Media Environment

The digital media environment has become increasingly vulnerable to diverse forms of cyber threats. Unlike conventional cyberattacks targeting financial institutions or government agencies, attacks against journalists frequently aim to suppress freedom of expression, compromise confidential sources, manipulate public discourse, or damage institutional credibility.

Common cyber threats affecting journalists include phishing campaigns, ransomware attacks, malware infections, account hijacking, identity theft, distributed denial-of-service (DDoS) attacks, surveillance, and unauthorized access to digital devices. Social engineering techniques have become particularly effective because they exploit human behavior rather than technical system vulnerabilities. Consequently, cybersecurity awareness plays a decisive role in reducing organizational and individual exposure to these threats.

Artificial intelligence has introduced both opportunities and challenges for cybersecurity within journalism. While AI-powered security systems improve threat detection and automated response capabilities, malicious actors increasingly employ artificial intelligence to generate sophisticated phishing campaigns, deepfake videos, automated misinformation, and highly convincing social engineering attacks. Sonni et al. (2024) demonstrated that AI-based security systems significantly improve the early detection of phishing attacks, whereas Korsgaard and Lehto (2022) emphasized the growing political and psychological influence of deepfake technologies in manipulating public opinion.

The widespread dissemination of misinformation and disinformation further complicates the cybersecurity landscape. Green and Luke (2019) argued that false information spreads rapidly across social media platforms, undermining public trust and increasing the burden on journalists responsible for verifying information under tight time constraints. Consequently, journalists must possess both digital literacy and cybersecurity competencies to distinguish authentic information from manipulated content.

2.3. Cybersecurity Awareness and Professional Journalism

Cybersecurity has become an essential component of responsible journalism. Protecting journalistic sources, confidential communications, unpublished materials, and digital identities requires both technological safeguards and informed professional practices.

International organizations increasingly recognize cybersecurity as an indispensable component of media resilience. According to the ITU (2023), strengthening cybersecurity awareness through continuous education and professional training represents one of the most effective approaches to reducing cyber vulnerabilities across institutions.

Within Arab countries, scholars have similarly emphasized the importance of cybersecurity awareness in enhancing digital resilience. Al-Buhairi (2023) argued that digital media can play a significant role in promoting cybersecurity culture and combating cybercrime through public awareness initiatives. Likewise, Yousfi and Massaoudi (2024) identified cybersecurity awareness as an essential

dimension of intellectual security, while Hassan (2021) highlighted cyberspace as an emerging domain requiring comprehensive security strategies.

Despite increasing scholarly attention to cybersecurity, empirical studies specifically investigating cybersecurity awareness among professional journalists remain limited, particularly within the Algerian context. Most existing research focuses on students, educational institutions, or general internet users rather than media professionals. This gap justifies the present study, which examines cybersecurity awareness among Algerian digital media journalists and evaluates its contribution to addressing cyber threats within professional journalistic practice.

3. Methodology

3.1. Research Design

This study employed a quantitative descriptive survey design to investigate the role of cybersecurity awareness in addressing cyber threats among digital media journalists in Algeria. The descriptive survey method was selected because it enables the systematic collection of data regarding participants' knowledge, attitudes, perceptions, and cybersecurity practices within their natural professional environment. This approach is particularly appropriate for examining current levels of cybersecurity awareness and identifying prevailing behavioral patterns among journalists.

3.2. Population and Sample

The target population consisted of journalists working in digital media organizations operating in Algeria, including online news platforms, digital newspapers, and multimedia news services.

A purposive sampling strategy was adopted to recruit participants who actively engage in digital journalism and regularly utilize online communication technologies in their professional activities. The final sample comprised 50 digital media journalists, representing diverse professional backgrounds and varying levels of experience within the Algerian media sector.

Participation in the study was voluntary, and all respondents provided informed consent prior to completing the questionnaire. Respondents were assured that their identities would remain anonymous and that the collected data would be used exclusively for academic research purposes.

3.3. Research Instrument

Data were collected using a structured online questionnaire developed based on previous cybersecurity awareness literature and studies addressing cyber threats within digital environments.

The questionnaire consisted of two sections.

The first section collected demographic information, including gender, age, educational qualification, professional experience, and workplace characteristics.

The second section measured cybersecurity awareness and cybersecurity-related practices through four dimensions:

- Awareness of cybersecurity concepts and principles;
- Awareness of cyber threats encountered in digital journalism;
- Adoption of cybersecurity practices and protective behaviors;
- Perceived contribution of cybersecurity awareness to preventing and mitigating cyber threats.

Responses were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

3.4. Validity and Reliability

Content validity was established through a comprehensive review of the relevant literature on cybersecurity awareness, digital journalism, and information security. The questionnaire items were designed to reflect the principal constructs identified in previous empirical studies.

To ensure internal consistency, the questionnaire should be evaluated using Cronbach's alpha coefficient. A coefficient of 0.70 or higher is generally considered indicative of acceptable reliability for social science research.

3.5. Data Collection Procedure

The questionnaire was distributed electronically using online survey software. Data collection was conducted during the first quarter of **2026**. Participants received an invitation explaining the objectives of the research, emphasizing voluntary participation and confidentiality.

Completed questionnaires were screened for completeness before statistical analysis.

3.6. Data Analysis

The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS).

Descriptive statistical techniques—including frequencies, percentages, means, and standard deviations—were employed to describe respondents' demographic characteristics and levels of cybersecurity awareness.

The findings are presented using tables and descriptive interpretations to evaluate journalists' awareness of cybersecurity, their adoption of secure digital practices, and their perceptions regarding the effectiveness of cybersecurity awareness in addressing cyber threats within the digital media environment.

3.7. Ethical Considerations

The study adhered to established ethical principles governing social science research. Participation was voluntary, respondents retained the right to withdraw at any stage without consequence, and no personally identifiable information was collected. All responses were treated confidentially and analyzed in aggregate form solely for academic purposes.

4. Significance of the Study

The increasing integration of digital technologies into journalistic practice has transformed the operational landscape of contemporary media while simultaneously exposing journalists and media organizations to a rapidly evolving spectrum of cyber threats. As digital news production becomes increasingly dependent on internet-based platforms, cloud services, mobile technologies, and social networking applications, cybersecurity has emerged as a fundamental requirement for ensuring the continuity, integrity, and credibility of journalistic work.

The significance of this study lies in its examination of cybersecurity awareness among digital media journalists in Algeria, a professional group that routinely handles sensitive information, communicates with confidential sources, and relies extensively on digital communication technologies. Despite the growing body of cybersecurity research, empirical studies investigating cybersecurity awareness within the journalism profession remain relatively scarce, particularly in the North African and Arab contexts. This study therefore contributes to addressing an important gap in the existing literature by providing empirical evidence regarding journalists' awareness of cyber threats and the protective practices they adopt in their professional activities.

From a theoretical perspective, the study contributes to the expanding interdisciplinary literature linking cybersecurity, digital communication, and journalism. It provides insights into how cybersecurity awareness influences journalists' perceptions of cyber risks and supports secure professional practices within digital media organizations.

From a practical perspective, the findings may assist media organizations, journalism schools, policymakers, and cybersecurity specialists in designing evidence-based training programs, awareness campaigns, and institutional cybersecurity policies. Strengthening cybersecurity awareness among journalists is expected to improve digital resilience, enhance the protection of confidential information and journalistic sources, reduce organizational vulnerabilities, and reinforce public trust in digital media institutions.

5. Objectives of the Study

The primary objective of this study is to investigate the role of cybersecurity awareness in addressing cyber threats within the Algerian digital media environment. Specifically, the study seeks to:

- assess the level of cybersecurity awareness among digital media journalists in Algeria;
- identify the cybersecurity practices adopted by journalists to protect digital information, communication channels, and confidential sources;
- examine the contribution of cybersecurity awareness to mitigating cyber threats and reducing cybersecurity risks within digital journalism;
- develop evidence-based recommendations that support the implementation of cybersecurity awareness programs and institutional security strategies for digital media organizations.

6. Research Methodology

This study employed a quantitative descriptive survey design, which is considered one of the most appropriate methodological approaches for investigating perceptions, attitudes, awareness, and behavioral practices within a defined population. The survey method enables researchers to collect standardized empirical data directly from participants, thereby facilitating the systematic analysis of cybersecurity awareness and professional security practices among journalists.

According to Barakat (2012), survey research is a scientific approach for collecting factual information and describing the characteristics of a phenomenon through data obtained from members of the target population. Given that the present study seeks to explore journalists' awareness of cybersecurity and their perceptions of cyber threats within the digital media environment, the survey method provides a reliable framework for achieving the study objectives.

Data were collected through a structured online questionnaire distributed electronically to digital media journalists working in Algeria. The questionnaire was designed to measure respondents' cybersecurity awareness, their understanding of cyber threats, and the protective measures they employ during their professional activities. The quantitative approach further allows the application of descriptive statistical techniques to identify prevailing patterns and trends within the collected data.

7. Study Population, Sampling Procedure, and Research Instrument

The target population comprised journalists employed in Algeria's digital media sector, including online newspapers, digital news websites, multimedia platforms, and electronic broadcasting organizations. Because no comprehensive database containing all digital journalists in Algeria was available, probability sampling techniques could not be employed.

Accordingly, the study adopted a purposive sampling strategy, whereby participants were intentionally selected based on characteristics directly relevant to the objectives of the research. To ensure the suitability of the respondents, participants were required to be actively employed within a digital media organization and possess at least one year of professional experience in digital journalism.

The final sample consisted of 50 digital media journalists representing various digital news organizations operating in Algeria.

Data were collected using a structured questionnaire developed through Google Forms and distributed electronically to participants. The questionnaire was constructed following an extensive review of previous literature on cybersecurity awareness, cyber threats, and digital journalism to ensure conceptual consistency and content validity. The instrument was designed to measure both cognitive and behavioral dimensions of cybersecurity awareness while maintaining clarity, simplicity, and ease of completion.

The questionnaire was organized into four analytical dimensions:

- Section I: Awareness of the concept, principles, and importance of cybersecurity among digital media journalists.
- Section II: Awareness of cyber threats and digital security risks encountered in the professional media environment.
- Section III: Cybersecurity practices adopted by journalists to protect digital identities, communication channels, confidential information, and journalistic sources.
- Section IV: Perceptions regarding the contribution of cybersecurity awareness to preventing, detecting, and mitigating cyber threats within digital journalism.

8. Theoretical Framework

8.1. Conceptualizing Cybersecurity

Cybersecurity has become one of the defining concepts of the digital age as governments, organizations, and individuals increasingly depend upon interconnected information and communication technologies. The expansion of digital infrastructures has generated unprecedented opportunities for communication and information exchange while simultaneously creating new categories of cyber risks capable of disrupting economic activities, governmental services, and professional communication.

Broadly defined, cybersecurity encompasses the technologies, policies, organizational procedures, legal frameworks, and human competencies designed to protect digital systems, communication networks, software applications, and information assets from unauthorized access, manipulation, disruption, or destruction. Its principal objective is to preserve the confidentiality, integrity, and availability of digital information while ensuring the resilience and continuity of technological systems.

Jabbour (2012) conceptualizes cybersecurity as a comprehensive activity intended to protect both human and financial resources associated with information and communication technologies while minimizing the consequences of cyber risks and restoring operational continuity following security incidents. Similarly, Amoroso describes cybersecurity as an integrated collection of technical measures and defensive mechanisms designed to reduce attacks targeting computer systems, software, and communication networks through encryption, intrusion detection, antivirus technologies, and other protective solutions (Tala, 2020).

The U.S. National Institute of Standards and Technology (NIST) further defines cybersecurity as the protection of computer systems, electronic communication services, communication infrastructures, and digital information against unauthorized access, disruption, manipulation, or destruction while preserving confidentiality, integrity, availability, authenticity, and resilience.

Within digital journalism, cybersecurity extends beyond technical protection. It encompasses safeguarding confidential journalistic sources, encrypted communications, unpublished investigations, digital identities, editorial infrastructure, and organizational reputation. Consequently, cybersecurity has become an essential professional competency supporting journalistic independence, ethical responsibility, and information integrity.

8.2. The Importance of Cybersecurity in Digital Media Organizations

The digital transformation of journalism has substantially increased the dependence of media organizations on internet-based technologies, cloud computing, mobile communication, and social networking platforms. Although these developments have enhanced news production and audience engagement, they have simultaneously expanded organizational exposure to cyber threats.

One of the primary functions of cybersecurity within media organizations is the protection of confidential journalistic sources and sensitive information. Unauthorized disclosure resulting from cyberattacks may compromise investigative reporting, endanger whistleblowers, and undermine journalistic credibility.

Cybersecurity also safeguards institutional reputation by preventing website defacement, account hijacking, data breaches, and the dissemination of manipulated information that may erode public trust. Because credibility represents one of the most valuable assets of journalism, effective cybersecurity has become an integral component of strategic media governance.

Equally important is ensuring operational continuity. Cyberattacks such as distributed denial-of-service (DDoS) attacks, ransomware, malware infections, and infrastructure compromise may interrupt news production and limit public access to reliable information during periods of social or political significance.

Digital media organizations also bear responsibility for protecting audience information, including subscriber data, personal identifiers, financial records, communication histories, and behavioral analytics. Robust cybersecurity practices are therefore essential for maintaining user privacy and complying with emerging data protection standards.

Furthermore, cybersecurity contributes to combating coordinated disinformation campaigns, malicious automated accounts, digital impersonation, and AI-generated synthetic media. As cyber threats continue to evolve in sophistication, cybersecurity must be regarded as a strategic organizational capability that strengthens the resilience, credibility, and long-term sustainability of digital journalism.

8.3. Cyber Threats in the Digital Media Environment

Concept of Cyber Threats

The accelerated digitalization of media ecosystems has substantially expanded the cybersecurity challenges confronting journalists and media organizations worldwide. As news production, editorial management, and audience engagement increasingly rely on interconnected digital technologies, cyber threats have evolved into one of the most significant risks affecting the security, credibility, and sustainability of digital journalism. Unlike conventional security threats, cyber threats transcend geographical boundaries, evolve rapidly, and exploit both technological vulnerabilities and human behavior to compromise information systems and communication networks (International Telecommunication Union [ITU], 2023; Kaspersky, 2024).

Cyber threats are generally defined as malicious activities conducted through information and communication technologies with the intention of compromising the confidentiality, integrity, or availability of digital information and technological infrastructures. Al-Buhairi (2023) describes cyber threats as attacks executed through modern digital technologies, electronic networks, and smart devices to steal sensitive information, disrupt communication systems, and damage digital infrastructure. Similarly, Ben Saber and Haidara (2017) define cyber threats as deliberate attempts to manipulate computer systems, infiltrate communication networks, and obtain unauthorized access to strategic information while impairing the operational capabilities of targeted systems.

Contemporary cybersecurity literature conceptualizes cyber threats as multidimensional phenomena that encompass technical attacks, social engineering, psychological manipulation, and information operations. Their consequences extend far beyond technological disruption, affecting institutional reputation, journalistic independence, democratic participation, and public confidence in media organizations (ITU, 2023; Kaspersky, 2024).

Within digital journalism, cyber threats represent a unique category of professional risk because journalists routinely handle confidential information, maintain communication with anonymous sources, and publish information with substantial social and political implications. Consequently, successful cyberattacks may not only compromise sensitive data but also threaten source confidentiality, interrupt editorial workflows, manipulate news content, and undermine the credibility of media institutions. Recent

reports indicate that journalists have increasingly become targets of sophisticated phishing campaigns, spyware, ransomware, surveillance technologies, and coordinated disinformation operations designed to influence public discourse and restrict press freedom (Kaspersky, 2024; Sonni et al., 2024).

Cyber threats are characterized by several distinctive features. They evolve continuously as attackers adopt increasingly sophisticated technologies, including artificial intelligence and automation. They can be launched remotely with minimal physical infrastructure, spread rapidly across interconnected digital systems, and simultaneously target multiple organizations and individuals. Moreover, cyberattacks frequently exploit human error rather than technical weaknesses, highlighting the importance of cybersecurity awareness as one of the most effective defensive mechanisms against cyber risks (Garcia & Bongo, 2022; ITU, 2023).

8.4. Major Cyber Threats Affecting Digital Media

The contemporary digital media environment is exposed to a wide spectrum of cyber threats that differ in their technical characteristics, operational objectives, and potential consequences. Collectively, these threats present substantial challenges to journalists, media organizations, and information security professionals.

Malware represents one of the most prevalent categories of cyber threats. Malware comprises malicious software intentionally designed to infiltrate digital devices, disrupt system functionality, steal information, or provide unauthorized access to attackers. Media organizations frequently encounter malware through infected email attachments, compromised websites, malicious advertisements, and manipulated multimedia files. Once installed, malware may compromise editorial systems, expose confidential journalistic information, or facilitate additional cyberattacks (Kaspersky, 2024).

Computer viruses constitute another significant cybersecurity threat. These self-replicating malicious programs attach themselves to legitimate files and spread throughout computer systems after activation. Virus infections may damage operating systems, corrupt digital archives, delete essential journalistic materials, and interrupt newsroom operations. Because digital journalism depends heavily upon continuous access to electronic information, virus outbreaks may significantly disrupt editorial productivity and information dissemination.

Ransomware has emerged as one of the most destructive forms of cybercrime targeting media organizations. Ransomware encrypts victims' digital files and demands financial payment in exchange for restoring access. Successful ransomware attacks may force media organizations to suspend publishing activities, interrupt newsroom operations, delay breaking news coverage, and incur substantial financial losses associated with system recovery and operational downtime (Kaspersky, 2024).

Phishing attacks remain among the most common attack vectors targeting journalists. Through fraudulent emails, deceptive websites, social media messages, or text messages, attackers attempt to persuade victims to disclose passwords, authentication credentials, financial information, or confidential organizational data. Because journalists routinely communicate with unfamiliar contacts and receive large volumes of electronic correspondence, phishing attacks represent a particularly serious professional risk (Hassan, 2021). Recent studies demonstrate that cybersecurity awareness and user education remain among the most effective strategies for reducing susceptibility to phishing attacks (Garcia & Bongo, 2022; Sonni et al., 2024).

Deepfake technologies have introduced a new generation of information security challenges within digital journalism. Advances in artificial intelligence and deep learning enable the creation of highly realistic synthetic videos, images, and audio recordings capable of convincingly imitating real individuals. These technologies can be exploited to disseminate misinformation, damage institutional reputations, manipulate political discourse, or undermine public trust in authentic journalistic content. As deepfake technologies become increasingly accessible, journalists must develop advanced digital verification skills alongside cybersecurity competencies (Korsgaard & Lehto, 2022).

Content manipulation and disinformation constitute another critical cyber threat affecting digital media. Coordinated campaigns involving fabricated news stories, manipulated images, automated social media accounts, and misleading narratives are increasingly employed to influence public opinion, distort political debates, and undermine confidence in legitimate news organizations. Green and Luke (2019) argue that misinformation spreads rapidly through digital platforms due to algorithmic amplification and high levels of user engagement, making verification processes considerably more challenging for professional journalists.

Increasingly, these threats no longer occur independently. Sophisticated cyber campaigns frequently combine phishing, malware, social engineering, artificial intelligence, and disinformation into coordinated attacks that simultaneously target technological infrastructure and human decision-making. Consequently, strengthening cybersecurity awareness has become a strategic necessity for media organizations seeking to enhance digital resilience and preserve journalistic integrity.

8.5. Cybersecurity Awareness

Cybersecurity awareness has emerged as a fundamental component of digital resilience in contemporary organizations. As cyber threats become increasingly sophisticated, technological solutions alone are insufficient to ensure information security. Human behavior is now widely recognized as one of the most critical determinants of organizational cybersecurity, making awareness, education, and secure digital practices essential components of comprehensive cybersecurity strategies (ITU, 2023).

Cybersecurity awareness generally refers to the level of knowledge, understanding, attitudes, and behavioral competencies that enable individuals to recognize cyber risks, evaluate potential security threats, and adopt appropriate protective measures during their interaction with digital technologies. Rather than representing purely technical expertise, cybersecurity awareness encompasses informed decision-making, responsible online behavior, and continuous vigilance against evolving cyber risks.

The International Telecommunication Union (2023) defines cybersecurity awareness as the collection of knowledge, skills, and behavioral competencies that enable individuals to identify cyber threats and implement appropriate protective measures to safeguard digital systems and information assets. Similarly, Garcia and Bongo (2022) conceptualize cybersecurity awareness as the integration of cybersecurity knowledge with practical behaviors that collectively reduce individuals' vulnerability to cyberattacks.

Recent research increasingly emphasizes the human dimension of cybersecurity. Studies indicate that a substantial proportion of successful cyberattacks originate from human error, including weak password practices, unsafe browsing behavior, failure to recognize phishing attempts, and inadequate protection of confidential information. Consequently, cybersecurity awareness programs seek not only to improve technical knowledge but also to cultivate secure behavioral habits that reduce organizational exposure to cyber risks (Garcia & Bongo, 2022; OPSWAT, 2023).

Within journalism, cybersecurity awareness assumes particular importance because media professionals routinely handle confidential sources, unpublished investigations, editorial communications, and sensitive organizational information. Journalists possessing higher levels of cybersecurity awareness are generally better equipped to identify suspicious online activities, implement secure communication practices, protect confidential information, and respond effectively to cyber incidents without compromising journalistic integrity.

For the purposes of the present study, cybersecurity awareness is operationally defined as the extent to which digital media journalists understand cybersecurity principles, recognize cyber threats associated with digital journalism, appreciate the importance of secure digital behavior, and implement appropriate cybersecurity practices to reduce their vulnerability to cyberattacks while protecting confidential information, journalistic sources, and digital media infrastructures.

9. Results

9.1. Awareness of the Concept and Importance of Cybersecurity among Digital Media Journalists

Table 3. Respondents' Awareness of the Concept of Cybersecurity

Response	Frequency	Percentage
Protecting information systems and data from cyberattacks	46	64%
Securing networks against cyber threats and cyber espionage	15	21%
Digital risk management	10	14%
Total*	**71**	**100%**

*Note. Respondents were permitted to select more than one response.

Table 3 presents respondents' understanding of the concept of cybersecurity. The findings reveal that the majority of participants (64%) identified cybersecurity primarily as the protection of information systems and digital data from cyberattacks. This result demonstrates that digital media journalists possess a strong awareness of the technical dimension of cybersecurity and recognize the importance of protecting digital infrastructures against unauthorized access and malicious attacks. Given the increasing dependence of journalism on digital technologies, this finding suggests that respondents appreciate cybersecurity as a fundamental mechanism for maintaining the confidentiality, integrity, and availability of journalistic information (ITU, 2023; Kaspersky, 2024).

Approximately one-fifth of respondents (21%) associated cybersecurity with protecting communication networks against cyber threats and cyber espionage. This finding indicates that journalists recognize the strategic importance of securing network infrastructure, particularly because contemporary news production relies heavily on cloud services, remote communication, and internet-based collaboration. Previous studies have similarly emphasized that securing communication networks is essential for protecting confidential journalistic sources and ensuring uninterrupted editorial operations (Sonni et al., 2024).

By comparison, only 14% of respondents viewed cybersecurity primarily as digital risk management. Although this proportion is considerably lower than those emphasizing technical protection, it nevertheless reflects an emerging understanding that cybersecurity also encompasses governance, organizational preparedness, and strategic risk mitigation. The relatively limited recognition of this managerial dimension suggests that journalists continue to perceive cybersecurity principally as a technological issue rather than as an integrated organizational process involving risk assessment, institutional policy, and crisis management. Similar observations have been reported in previous cybersecurity awareness studies, which found that end users generally demonstrate stronger familiarity with technical threats than with broader cybersecurity governance frameworks (Garcia & Bongo, 2022; ITU, 2023).

Overall, the findings indicate that respondents possess a satisfactory conceptual understanding of cybersecurity. Nevertheless, strengthening awareness regarding cybersecurity governance, digital risk management, and organizational resilience may further enhance journalists' ability to address increasingly sophisticated cyber threats within digital media environments.

Table 4. Respondents' Awareness of the Importance of Cybersecurity

Response	Frequency	Percentage
Protecting digital assets and sensitive journalistic information	23	24%
Combating misinformation and fake news while ensuring media credibility	27	28%
Preserving the credibility and reputation of media organizations	20	21%
Protecting journalists from hacking, cyber espionage, and surveillance	25	26%
Total*	**95**	**100%**

*Note. Respondents were permitted to select more than one response.

The results presented in Table 4 demonstrate that respondents possess a multidimensional understanding of the significance of cybersecurity within digital journalism. The largest proportion of participants (28%) considered combating misinformation and fake news while preserving the credibility of media content to be the most important function of cybersecurity. This finding reflects growing recognition that cybersecurity extends beyond protecting technical infrastructure and plays a crucial role in safeguarding information integrity and maintaining public trust in digital media. The proliferation of coordinated disinformation campaigns, AI-generated content, and manipulated digital information has significantly increased the importance of cybersecurity within contemporary journalism (Green & Luke, 2019; Korsgaard & Lehto, 2022).

The second highest proportion of respondents (26%) emphasized the importance of protecting journalists from hacking, cyber espionage, and digital surveillance. This finding is particularly significant because journalists increasingly become targets of sophisticated cyberattacks intended to compromise confidential communications, reveal anonymous sources, or disrupt investigative reporting. International cybersecurity reports consistently identify journalists as one of the professional groups most exposed to cyber espionage and targeted phishing campaigns (Kaspersky, 2024; ITU, 2023).

Nearly one-quarter of respondents (24%) identified the protection of digital assets and sensitive journalistic information as the primary importance of cybersecurity. This result reflects respondents' awareness that digital archives, editorial documents, unpublished investigations, and confidential communications constitute valuable organizational assets requiring comprehensive protection against unauthorized access and data breaches.

Meanwhile, 21% of respondents emphasized cybersecurity's role in protecting the reputation and institutional credibility of media organizations. This finding is consistent with previous research demonstrating that successful cyberattacks, website compromise, and dissemination of manipulated information may substantially damage organizational reputation, reduce audience trust, and undermine journalistic legitimacy (Al-Buhairi, 2023; Sonni et al., 2024).

Taken together, these findings indicate that digital media journalists perceive cybersecurity as an integrated professional responsibility encompassing information protection, institutional resilience, media credibility, and journalist safety. Such a comprehensive understanding provides a favorable foundation for implementing cybersecurity awareness initiatives within digital media organizations.

9.2. Awareness of Cyber Threat Risks among Digital Media Journalists

Table 5. Respondents' Awareness of Cyber Threat Risks

Statement	Frequency	Percentage
I am familiar with the different types of cyber threats affecting digital journalists.	46	20%
I recognize the risks associated with digital account compromise affecting journalists and media organizations.	42	18%
I am aware of the risks posed by malware to devices used in journalistic work.	39	16%
I understand the impact of Distributed Denial-of-Service (DDoS) attacks on digital media websites.	36	15%
I recognize the dangers of deepfake technologies in spreading misinformation.	40	17%
I am aware of the risks associated with the leakage of sensitive journalistic information.	34	14%
Total*	**237**	**100%**

*Note. Respondents were permitted to select more than one response.

Table 5 illustrates respondents' awareness of the principal cyber threats confronting digital journalism. Overall, the findings reveal a relatively balanced distribution across all identified threat categories, suggesting that participants possess broad rather than selective cybersecurity knowledge.

The highest proportion of respondents (20%) reported familiarity with the various forms of cyber threats targeting digital journalists. This finding demonstrates that respondents possess a general understanding of the cybersecurity landscape affecting contemporary journalism and recognize that cyber threats have become an inherent component of digital media practice. Previous studies similarly conclude that awareness of cyber risks represents one of the strongest predictors of secure online behavior and effective cybersecurity decision-making (Garcia & Bongo, 2022; ITU, 2023).

Approximately 18% of respondents recognized the risks associated with unauthorized access to journalists' and media organizations' digital accounts. This finding reflects awareness of one of the most common attack vectors employed by cybercriminals. Account compromise frequently enables attackers to access confidential communications, manipulate published content, impersonate journalists, or obtain sensitive editorial information. Consequently, protecting digital identities has become a critical component of professional cybersecurity within journalism (OPSWAT, 2023).

A further 17% of respondents acknowledged the growing dangers posed by deepfake technologies. Artificial intelligence has significantly enhanced the realism of synthetic audio and video content, thereby increasing the potential for misinformation, reputational attacks, and political manipulation. This finding supports the conclusions of Korsgaard and Lehto (2022), who demonstrated that deepfake technologies substantially undermine public trust in digital media while increasing skepticism toward authentic journalistic content.

Regarding malware, 16% of respondents reported awareness of its potential impact on journalistic work. Malware remains one of the most common cyber threats affecting media organizations because it enables attackers to steal information, monitor user activities, encrypt digital files, or establish persistent unauthorized access to organizational systems (Kaspersky, 2024).

Similarly, 15% of respondents recognized the consequences of Distributed Denial-of-Service (DDoS) attacks for digital media organizations. Such attacks can temporarily disable news websites, interrupt public access to information, and significantly disrupt newsroom operations, particularly during periods of heightened political or social importance.

Although the lowest proportion of respondents (14%) referred to the risks associated with the leakage of confidential journalistic information, the finding nevertheless demonstrates awareness of the importance of protecting sensitive documents, confidential sources, unpublished investigations, and organizational communications. Given the central role of source confidentiality in investigative journalism, enhancing awareness of information protection remains an important priority for media organizations.

Overall, the relatively small variation across response categories indicates that respondents demonstrate a comprehensive understanding of the diverse cyber threats confronting digital journalism. This balanced awareness suggests that cybersecurity education among digital journalists extends beyond individual attack techniques and encompasses a broader appreciation of the evolving cyber threat landscape. The findings further support previous international research emphasizing that cybersecurity awareness constitutes a fundamental

prerequisite for strengthening journalists' digital resilience and reducing organizational exposure to cyber risks (ITU, 2023; Sonni et al., 2024; Kaspersky, 2024).

9.3. Cybersecurity Practices Adopted by Digital Media Journalists

Table 6. Cybersecurity Practices Adopted by Respondents

Security Practice	Frequency	Percentage
Using strong and unique passwords for professional accounts	47	20%
Verifying suspicious links and email attachments before opening them	42	18%
Maintaining backup copies of important journalistic data	41	17%
Using encrypted communication tools when communicating with sensitive sources	38	16%
Regularly updating operating systems and software	35	15%
Knowing the procedures to follow after detecting a cybersecurity incident	32	13%
Total*	**235**	**100%**

*Note. Respondents were permitted to select more than one response.

Table 6 presents the cybersecurity practices implemented by digital media journalists during their professional activities. Overall, the findings indicate that respondents have adopted several preventive cybersecurity measures, although the degree of implementation differs across practices.

The most frequently reported practice was the use of strong and unique passwords for professional accounts (20%). This finding suggests that respondents recognize password security as the first line of defense against unauthorized access to digital accounts and journalistic information. Password management remains one of the most effective and cost-efficient cybersecurity controls because compromised credentials continue to account for a substantial proportion of cyber incidents worldwide. According to Verizon's *Data Breach Investigations Report*, credential compromise remains among the leading causes of successful cyberattacks, emphasizing the importance of robust authentication mechanisms (Verizon, 2024). Similarly, OPSWAT (2023) recommends the adoption of strong passwords, password managers, and multi-factor authentication as essential cybersecurity practices.

The second most frequently reported behavior involved verifying suspicious hyperlinks and email attachments before opening them (18%). This preventive practice demonstrates respondents' awareness of phishing attacks, which continue to represent one of the most common entry points for malware infections, credential theft, and ransomware attacks targeting media organizations. Previous studies indicate that cybersecurity awareness significantly reduces individuals' susceptibility to phishing campaigns because informed users are more likely to recognize fraudulent communications before interacting with malicious content (Garcia & Bongo, 2022; Sonni et al., 2024).

Approximately 17% of respondents reported maintaining backup copies of important journalistic documents and digital information. Regular data backup is widely recognized as a fundamental component of organizational cyber resilience because it enables media organizations to restore critical information following ransomware attacks, system failures, or accidental data loss. For digital journalism, preserving editorial archives, investigative materials, and confidential documents is essential for ensuring operational continuity and protecting institutional memory (Kaspersky, 2024).

The use of encrypted communication tools when communicating with confidential sources was reported by 16% of respondents. This finding reflects awareness of the ethical and professional obligation to protect source confidentiality, which remains one of the defining principles of investigative journalism. Secure communication platforms employing end-to-end encryption significantly reduce the risk of unauthorized interception and surveillance while strengthening journalists' ability to safeguard sensitive information (ITU, 2023).

Regular software and operating system updates were reported by 15% of participants. Although software updates represent a relatively simple cybersecurity measure, they remain one of the most effective methods for addressing known security vulnerabilities before they can be exploited by malicious actors. Maintaining updated systems therefore contributes directly to reducing organizational exposure to cyber threats.

The least frequently reported practice (**13%**) concerned respondents' familiarity with **incident response procedures** following the detection of a cybersecurity breach. Although respondents generally demonstrated satisfactory preventive cybersecurity behavior, this finding suggests comparatively limited preparedness regarding post-incident response and organizational crisis management. Previous

research consistently emphasizes that effective cybersecurity depends not only upon prevention but also upon the existence of clearly defined response protocols capable of minimizing operational disruption following cyber incidents (NIST, 2024; ITU, 2023).

Overall, the findings indicate that respondents demonstrate a satisfactory level of cybersecurity practice within their professional activities. Nevertheless, strengthening incident response capabilities, organizational preparedness, and cybersecurity governance should remain priorities for digital media organizations seeking to improve institutional resilience against increasingly sophisticated cyber threats.

9.4. Perceived Contribution of Cybersecurity Awareness to Addressing Cyber Threats

Table 7. Respondents' Perceptions of the Contribution of Cybersecurity Awareness

Response	Frequency	Percentage
Protecting sensitive data and professional information from cyber intrusions	45	29%
Enhancing the early detection of cyber threats	40	25%
Maintaining business continuity and uninterrupted information flow	38	24%
Strengthening public trust in digital media content	34	22%
Total*	**157**	**100%**

*Note. Respondents were permitted to select more than one response.

The findings presented in Table 7 demonstrate that respondents perceive cybersecurity awareness as a strategic component of digital journalism rather than merely a technical requirement.

The largest proportion of respondents (29%) considered cybersecurity awareness essential for protecting sensitive information and professional journalistic data against cyber intrusions. This finding reflects widespread recognition that journalists routinely process confidential documents, unpublished investigations, and sensitive communications requiring comprehensive digital protection. Similar conclusions have been reported by Yousfi and Massaoudi (2024), who argue that cybersecurity awareness strengthens information security by reducing organizational vulnerabilities and enhancing protection against cyberattacks.

Approximately 25% of respondents believed that cybersecurity awareness contributes to the early identification of cyber threats. Early detection constitutes one of the principal objectives of modern cybersecurity because timely recognition enables organizations to implement preventive measures before cyber incidents escalate into significant operational disruptions. Recent advances in artificial intelligence have further strengthened early detection capabilities by enabling automated identification of anomalous behavior, malicious network traffic, and phishing campaigns through machine learning algorithms (Sonni et al., 2024).

Nearly one-quarter of respondents (24%) emphasized the role of cybersecurity awareness in maintaining operational continuity and ensuring uninterrupted information dissemination. Digital journalism depends upon continuous system availability, and cyber incidents capable of disrupting editorial workflows may prevent timely communication with the public. Consequently, cybersecurity awareness contributes not only to technical protection but also to organizational resilience and service continuity.

The remaining 22% of respondents highlighted cybersecurity awareness as an important factor in strengthening public trust in digital media content. This finding illustrates that respondents recognize the close relationship between cybersecurity, information integrity, and institutional credibility. Cyberattacks involving manipulated content, unauthorized publication, or coordinated disinformation campaigns can substantially reduce audience confidence in media organizations. Accordingly, cybersecurity has become an essential component of preserving journalistic credibility and protecting democratic information environments (Green & Luke, 2019; Korsgaard & Lehto, 2022).

Collectively, these findings indicate that respondents perceive cybersecurity awareness as extending well beyond technical system protection. Instead, it is viewed as a strategic organizational capability supporting information security, operational resilience, professional ethics, media credibility, and the long-term sustainability of digital journalism.

10. Discussion of Findings

The findings of the present study demonstrate that digital media journalists in Algeria possess a generally satisfactory level of cybersecurity awareness and recognize cybersecurity as an essential component of professional journalistic practice. Respondents exhibited relatively balanced knowledge across different dimensions of cybersecurity, including conceptual understanding, awareness

of cyber threats, implementation of preventive security measures, and appreciation of cybersecurity's contribution to strengthening organizational resilience.

The results further reveal that higher levels of cybersecurity awareness are accompanied by the adoption of practical cybersecurity behaviors such as password protection, verification of suspicious communications, secure handling of confidential information, and data backup. These findings are consistent with previous empirical research demonstrating that cybersecurity awareness positively influences secure online behavior and reduces organizational exposure to cyber risks (Garcia & Bongo, 2022; ITU, 2023).

At the same time, the comparatively limited awareness regarding cybersecurity incident response procedures suggests that future awareness initiatives should move beyond basic preventive practices toward comprehensive organizational preparedness. Contemporary cybersecurity frameworks emphasize that prevention, detection, response, and recovery should function as integrated components of organizational cyber resilience rather than independent activities (NIST, 2024).

11. Conclusion

The rapid digital transformation of journalism has fundamentally altered both the opportunities and the risks associated with contemporary media practice. As cyber threats continue to increase in sophistication, cybersecurity awareness has become an indispensable professional competency enabling journalists to protect confidential information, preserve source confidentiality, maintain operational continuity, and uphold the credibility of digital journalism.

The findings of this study demonstrate that digital media journalists in Algeria possess a generally high level of cybersecurity awareness and recognize the strategic importance of cybersecurity in protecting journalistic activities from cyber threats. Respondents reported implementing a range of preventive cybersecurity practices while acknowledging the significant contribution of cybersecurity awareness to strengthening digital resilience, improving threat detection, and safeguarding sensitive information.

These findings reinforce the growing consensus within the cybersecurity literature that technological solutions alone cannot adequately protect digital organizations. Instead, organizational resilience depends equally upon informed human behavior, continuous professional education, institutional cybersecurity culture, and effective governance mechanisms.

Recommendations

Based on the findings of this study, the following recommendations are proposed:

- Develop continuous cybersecurity education and certification programs specifically designed for digital journalists and newsroom personnel.
- Integrate cybersecurity, digital risk management, and secure communication practices into journalism curricula and professional development initiatives.
- Establish institutional cybersecurity policies, incident response protocols, and regular cybersecurity awareness campaigns within digital media organizations.
- Strengthen collaboration between media organizations, cybersecurity agencies, universities, and technology providers to exchange expertise and improve organizational resilience.
- Encourage media organizations to adopt artificial intelligence–based cybersecurity solutions capable of supporting threat intelligence, anomaly detection, phishing prevention, and automated verification of manipulated digital content.
- Promote regular cybersecurity risk assessments, penetration testing, and organizational security audits to identify vulnerabilities before they are exploited by malicious actors.

Declarations

Ethics Approval and Consent to Participate

This study was conducted in accordance with the ethical principles governing social science research. Participation in the survey was voluntary, and informed consent was obtained electronically from all participants prior to completing the questionnaire. Respondents were informed of the purpose of the study, assured of the confidentiality and anonymity of their responses, and advised that they could withdraw from the study at any stage without consequence. No personally identifiable information was collected or disclosed.

Consent for Publication

Not applicable.

Availability of Data and Materials

The datasets generated and analyzed during the current study are available from the corresponding author upon reasonable request. The data are not publicly available because they contain information that could potentially compromise participant confidentiality.

Competing Interests

The author declares that there are no financial or non-financial competing interests related to this research.

Funding

This research received no external funding.

Authors' Contributions

Nassima Lounis solely conceived and designed the study, developed the research instrument, collected and analyzed the data, interpreted the findings, conducted the literature review, and wrote, revised, and approved the final manuscript.

Acknowledgements

The author gratefully acknowledges all digital media journalists who voluntarily participated in this study by completing the questionnaire. Their valuable contributions made this research possible.

Authors' Information

Nassima Lounis is affiliated with the Faculty of Information and Communication Sciences, University of Algiers 3, Algeria. Her research interests include digital media, journalism studies, cybersecurity, media communication, digital transformation, and information security.

AI Statement

The author declares that any artificial intelligence (AI)-assisted technologies used during the preparation of this manuscript were employed solely to improve language quality, grammar, readability, and manuscript organization. The author takes full responsibility for the accuracy, originality, interpretation, and integrity of all content presented in this article.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to ethical and confidentiality considerations.

Conflict of Interest Statement

The author declares that there are no conflicts of interest regarding the publication of this paper.

References:

1. Al-Buhairi, S. (2023). The role of digital media in promoting cybersecurity and combating cyber threats and cybercrime. *Scientific Journal of Public Relations and Advertising Research*, *(25)*, 65.
2. Al-Shaiti, I. (2019). *Evaluation of information security and privacy policies in educational institutions in the Kingdom of Saudi Arabia: An applied study at Qassim University* (Unpublished master's thesis). Qassim University.
3. Barakat, A. A. (2012). *Media research methods: Theoretical foundations and practical application skills* (1st ed.). Dar Al-Kitab Al-Hadith.
4. Ben Saber, B., & Haidara, M. (2017). Cyber attacks and their confrontation in light of contemporary international law. *Journal of Human Rights and Public Freedoms*, *2*(4), 189.
5. Garcia, A. B., & Bongo, S. M. C. (2022). Cybersecurity cognizance among college teachers and students in embracing online education. In *Proceedings of the International Conference on Information Management* (p. 116).
6. Green, M., & Luke, S. (2019). The spread and impact of misinformation on social media. *Journal of Communication Studies, 45*(3), 121–135.
7. Hassan, H. (2021). Cyberspace and the challenges of global security. *Journal of Legal and Political Sciences, 12*(1), 69.
8. International Telecommunication Union. (2023). *Global cybersecurity index 2023*. https://www.itu.int/
9. Jabbour, M. A. (2012). *Cybersecurity: Challenges and requirements for confrontation*. Arab Center for Legal and Judicial Research.
10. Kaspersky. (2024). *Global cyber threat report*. Kaspersky.

11. Korsgaard, H. D., & Lehto, L. (2022). The psychological and political impact of deepfake videos on public opinion. *Journal of Social Media Studies, 7*(2), 189–206.
12. OPSWAT. (2023, May 4). *World Password Day: 6 ways to strengthen password security*. http://arabic.opswat.com/blog/2023-word-password-day-6-ways-to-strengthen-password-security
13. Sonni, F., Ibrahimi, A., & Elouaai, F. (2024). The role of artificial intelligence in detecting and preventing cyber and phishing attacks. *International Journal of Advanced Computer Science and Applications, 15*(1), 112–120.
14. Tala, L. (2020). Cyber threats and cybercrime: Their impact on national security and strategies for combating them. *Ma'alem Journal of Legal and Political Studies, 4*(2), 60.
15. Yousfi, S., & Massaoudi, K. (2024). Intellectual security and the challenges of cybersecurity: A theoretical study. *Al-Bahith Journal, 16*(2), 647–668.