International Journal of Educational Sciences and Arts (IJESA)
Vol. (4), No. (9)
IJESA
September 2025
المجلة الدولية للعلوم التربوية والآداب
الإصدار (4)، العدد (9)

The role of digital media in enhancing awareness of cybersecurity threats: An applied study on a sample of employees in the banking sector in the Kingdom of Bahrain

SH. Maryam Mubarak Alkhalifa
PhD Researcher in Digital Media and Communication Technology, Ahlia University, Kingdom of Bahrain
Mariamalkhalifa@hotmail.com

Abstract

This study aimed to evaluate the relationship between the roles of digital media and its ability to enhance awareness of cybersecurity threats in the banking sector in the Kingdom of Bahrain. This study employed a descriptive method and relied on a questionnaire as a data collection tool from a sample of the study. The researcher formulated a questionnaire consisting of 20 items in addition to the demographic data of the participants. The study sample comprised 400 participants from the banking sector in the Kingdom of Bahrain, which was divided into an exploratory sample of 35 participants and a main sample of 365 participants. This sample was collected intentionally. Through statistical analysis, the study reached a set of results, the most important of which is that employees in the banking sector in the Kingdom of Bahrain have a high level of awareness of cybersecurity threats that could disrupt the services provided by banks and represent a danger to the confidentiality of customer data and their banking transactions. Digital media, through its various means, plays important roles in raising awareness among banking sector employees to enhance cybersecurity.

One of the most prominent roles is to enhance the awareness of workers in the banking sector about the importance of protecting personal information and

customers' banking data. There is a statistically significant relationship between the digital media used in banks and the level of awareness among employees about countering cyber-attacks. There are no statistically significant differences in the opinions of banking sector employees regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to variables (gender - age - position - type of bank). It has been recommended to employ digital media more effectively to simplify the digital content published about cybersecurity and make it more engaging and interesting. It has also been suggested that there should be interaction with the digital content published about the cyber threats faced by banks and inquiring with specialists about the nature of threats that are difficult to understand.

Keywords: Media, Digital Media, Cybersecurity

Introduction

Although the technological development and the information and communication revolution that the world has witnessed for no less than three decades have produced many positive effects on society and its individuals and institutions, they have simultaneously generated unprecedented security threats. These technologies have allowed for the infringement on the personal information of individuals and institutions, and to execute attacks that jeopardize everyone's privacy, which are referred to as cyber-attacks. The danger of these attacks lies in their ability to disrupt the electronic systems of institutions that are directly linked to the national security of states. In order to confront these threats, the concept of cybersecurity has emerged, which is currently one of the most important forms of security that must be ensured.

The issue of cybersecurity and related information security concerns has emerged as an inevitable consequence of significant technological advancement, especially since the beginning of the third millennium. Cybersecurity and its threats have become a problem that worries everyone, including businesspeople, managers, security

experts, media professionals, economists, and anyone with important information. One of the most prominent sectors exposed to cybersecurity threats is the banking sector, which is considered the primary support for national economies, managing the accounts of individuals and institutions of various sizes. The financial data held by this sector is a target for cybercriminals. The banking sector has been suffering from a crisis of trust with the public following the financial crisis that the world witnessed in 2008, which was a direct outcome of banking practices that lacked transparency, accuracy, and integrity. It has become essential for this vital sector to regain the public's trust, leading experts in this sector to prioritize cybersecurity at the top of their concerns.

For this vital sector to regain public trust, cybersecurity must be placed at the top of the priorities by specialists in the sector. To increase the effectiveness of efforts made to achieve cybersecurity in the banking sector, the importance of raising awareness about cybersecurity practices among employees in this sector becomes evident. Available literature on enhancing employee awareness in achieving cybersecurity in the banking sector emphasizes that there are several knowledge gaps that both senior management and cybersecurity specialists need to address in order to build successful digital banking institutions in an economy based on trust and confidence. These gaps refer to four factors: commitment and support from senior management; budget; compliance with cybersecurity; and cybersecurity culture. (Al-Alawi & Al-Bassam, 2019)[1]

The importance of this research lies in understanding the role of digital media in raising awareness about cybersecurity threats in the banking sector in the Kingdom of Bahrain, as the banking sector in the Kingdom of Bahrain is a key partner in the success of the country in achieving its developmental goals and its economic vision

[1] Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. Arab Gulf Journal of Scientific Research, 37(4), 17-32.

for 2030. According to statistics from the central bank, this sector contributes approximately 17% annually to the national income of the Kingdom of Bahrain. (CBB, 2024)[2]

This sector faces serious cyber threats that jeopardize customer trust in banks and affect the banking sector's ability to manage banking operations and maintain the confidentiality of the data under its control. To mitigate the seriousness of cyber threats, it is not enough to rely solely on the cybersecurity practices implemented by banking departments; there must be a central role for employees, which requires enhancing awareness of these practices and how to address cybersecurity threats.

Digital media represents an indispensable tool in the banking sector, as reliance on digital communication tools in banks has increased due to the widespread availability and ease of use of these tools that have become accessible to everyone. Digital media helps employees to understand the essential procedures necessary to achieve cybersecurity, and they are informed about the key precautions to avoid when dealing with the sensitive data held by this sector.

This research focuses on the role of digital media in enhancing awareness of cybersecurity threats by applying it to a sample of employees in the banking sector in the Kingdom of Bahrain. It assesses the effectiveness of digital media in the banking sector in Bahrain and the extent to which banks can enhance their employees' awareness of the cyber risks and threats facing the banking sector. Studying these variables contributes to determining the banks' ability to confront the increasing threats to their cybersecurity in the Kingdom of Bahrain.

[2] Fact Sheet | CBB. (2024). Retrieved from www.cbb.gov.bh website: https://www.cbb.gov.bh/fact-sheet/

Research Problem

Banks are among the most susceptible institutions to cyber threats. With the vast amounts of sensitive data and financial transactions that occur daily, they become an attractive target for hackers. Cybersecurity in the banking sector has become the first line of defense against a growing wave of digital threats. It can be said that banks face constant pressure to stay one step ahead of cybercriminals. Here, the role of employees in this sector becomes prominent, as they represent the most important asset of the banking sector. Raising awareness among employees about cybersecurity threats and how to address them becomes crucial. The importance of digital media tools is manifested in what banks do to raise awareness among employees in the banking sector.

Here lies the problem of the research plan, which will focus on answering the main question: **What is the role of digital media in enhancing the awareness of employees about cybersecurity threats in the banking sector in the Kingdom of Bahrain?**

Research Questions

1. How aware are banking sector employees of cybersecurity threats?
2. What are the most influential digital means in promoting cybersecurity awareness?
3. What are the challenges of digital media in enhancing cybersecurity awareness in the banking sector?
4. What are the roles of digital media in educating banking sector employees about enhancing cybersecurity?
5. Is there a statistically significant relationship between the digital media used in banks and the level of awareness among employees to counter cyber-attacks?
6. Are there statistically significant differences in the opinions of employees in the

banking sector regarding the role of digital media in enhancing awareness of cybersecurity threats, attributed to variables (gender - age - job - type of bank)?

Research Hypotheses

1. There is a statistically significant relationship between the digital media used in banks and the level of awareness of employees in countering cyber-attacks.
2. There are statistically significant differences in the opinions of employees in the banking sector regarding the role of digital media in enhancing awareness of cybersecurity threats: attributed to variables (gender - age - position - type of bank).

Research Objectives

1. Measuring the extent of awareness among bank employees about cybersecurity threats.
2. Identifying the most effective digital means for enhancing cybersecurity awareness.
3. Recognizing the roles of digital media in educating bank employees about strengthening cybersecurity.
4. Assessing the challenges of digital media in enhancing awareness of cybersecurity in the banking sector.
5. Measuring the relationship between digital media used in banks and the level of awareness of employees in countering cyber-attacks.
6. Evaluating the existence of statistically significant differences between the opinions of employees in the banking sector regarding the role of digital media in raising awareness of cybersecurity threats: attributed to variables (gender - age - educational level - job - years of experience).

Research Concepts and Terms

In terminology, **media** refers to "all forms of communication activities aimed at providing the public with all facts, accurate news, and correct information about issues, topics, problems, and developments in an objective manner without distortion, contributing to the greatest possible degree of awareness, knowledge, understanding, and comprehensive insight among the public".

(Hossam,2022, p.7)[3]

In procedural terms, media is "the process through which information about a specific topic is gathered and transmitted to a specific audience through various means to achieve goals that include informing, educating, entertaining, or influencing public attitudes and opinions."

Digital media is defined as: "a set of new digital methods and activities through which media content can be produced, published, and exchanged in various forms in an interactive process between the sender and the recipient." (Qouich,2017, p.273)[4]

Digitally, the media is "those media activities that are carried out through modern technologies to convey information, news, and messages to the targeted audiences through various digital platforms such as social media."

Cybersecurity, by definition, is the act of protecting systems, networks, and programs from digital attacks that aim to access, alter, or destroy sensitive information, or to extort money from users. (Al-Omari, 2022, p.11)[5]

[3] Hossam, Mansour. (2022). Digital Media: Its Concept, Means, Theories, Journal of Research and Studies in New Media, (3)2.
[4] Qouich, Jamal al-Din, (2017) Media Education and Digital Media: A Study on Challenges and Strategies, Al-Risala Journal for Human Studies and Research, (2)3.
[5] Al-Omari, Hamad. (2022). Management of Cyber Crises and Their Impact on Bahraini National Security: A Practical Study in Light of the Cybersecurity Strategy of the Kingdom of Bahrain, Master's Thesis, Royal Police Academy, Kingdom of Bahrain.

Cybersecurity operationally: is the measures adopted by individuals or institutions to protect networks, information technology systems, operational technology systems, their components of hardware and software, services provided, and the data contained within these networks against any breaches, disruptions, or unlawful exploitation.

Literature Review

1- Al-Tamimi's study (2024) titled "The Role of Digital Media in Raising Awareness of the Risks of Cyber Crimes."[6]

This study aimed to assess the main risks associated with the increase of cybercrimes in society, to clarify the relationship between digital media and awareness of cybercrime risks, in addition to presenting the future outlook for the role of digital media in raising awareness of cybercrime risks. The study used a descriptive analytical approach and relied on a questionnaire to collect data on the subject of the study from a group of specialists in the media field in the Kingdom of Bahrain, specifically in television journalism and Bahraini radio. The study collected its data from a sample that included 45 participants.

The study concluded with several important findings, most notably that the characteristics of digital media enhance its effectiveness and impact in the modern media landscape through direct interaction, the ability to provide customized content, and rapid dissemination, leading to fundamental changes in how information is consumed and how individuals interact with media content. It is also concluded that the increase in cybercrimes leads to a rise in risks associated with personal data and lowers the level of trust in digital systems. The study showed that there is a positive relationship between digital media and improving individuals' awareness of the risks

[6] Al-Tamimi, Abdulaziz. (2024). The Role of Digital Media in Raising Awareness of the Risks of Cyber Crimes, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia.

of cybercrimes. Finally, the study confirmed that successive technological developments can enhance the role of digital media in raising awareness of the risks of cybercrimes.

2- The study by Al-Qahtani et al. (2024) titled "The Role of Saudi Digital Media in Raising Citizen Awareness of Cybercrime Technologies in the Kingdom of Saudi Arabia."[7]

This study highlighted the impact of digital media in the Kingdom of Saudi Arabia on raising citizens' awareness of cybercrimes and the techniques employed by criminals to commit these crimes. This study used a survey methodology, utilizing a questionnaire as a tool to collect data from a sample of 200 citizens from the Saudi community.

The study reached a number of findings, the most important of which is that the citizens of the Kingdom of Saudi Arabia are interested in learning about the main mechanisms used in the execution of cybercrimes in Saudi society. Understanding these mechanisms helps citizens to increase their awareness of these crimes and work to avoid them as much as possible, as the usual victims of these crimes are individuals who have no idea how they are carried out.

The study's results also confirmed that social media platforms are the most commonly used channels by criminals to carry out their electronic crimes, particularly WhatsApp, followed by Snapchat and X platform (formerly Twitter). The study's findings emphasize that Saudi governmental platforms provide the most support in combating electronic crimes.

[7] Al-Qahtani, Al-Lulu, Al-Mutairi, Shaqra Muhammad, and Al-Juhani, Amani Saleh. (2024). The role of Saudi digital media in raising citizens' awareness about cybercrime techniques in the Kingdom of Saudi Arabia (Field Study), Journal of Arts, Literature, Humanities and Social Sciences, 2024 (104).

3- Study by Wang, et al., (2024) titled "Data privacy and cybersecurity challenges in the digital transformation of the banking sector".[8]

This study aimed to shed light on the challenges faced by banks regarding data security and privacy during the digital transformation. It also focused on exploring the relationship between new technology, privacy, and data security. The study utilized a descriptive analytical approach and relied on literature review tools and analysis of relevant case studies in the banking sector.

The study also collected data from scientific articles, institutional reports, and specialized technical sources. It concluded that digital transformation increases cybersecurity risks, such as ransomware attacks and large data leaks. Moreover, weak security systems and excessive reliance on new technologies increase complexities. It emphasized that improving the awareness of bank employees is considered one of the best cybersecurity practices.

4- Study by Hassan, et al. (2024) titled: "Cybersecurity in banking: a global perspective with a focus on Nigerian practices".[9]

The study aimed to assess the challenges of cybersecurity in the banking sector at a global level, highlighting practices in Nigeria. It also sought to analyze strategies for addressing these challenges, evaluate the relationship between rapid digitalization and the increase in cyber threats, as well as identify vulnerabilities in current systems and propose solutions to enhance cybersecurity.

The study used a descriptive analytical approach, relying on the review of literature and reports related to cybersecurity in banks in Nigeria. The study reached several

[8] Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & Security, 147, 104051.
[9] Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41-59.

important findings, including an increase in cyberattacks such as phishing and ransomware in Nigeria, a lack of security awareness among customers, insufficient training for employees, and vulnerabilities in digital infrastructure and regulatory laws.

5- Al-Buhairi's study (2023) titled: "The Role of Digital Media in Enhancing Cybersecurity and Combating Cyber Threats and Crimes".[10]

This study aimed to identify the role played by digital media in enhancing and combating cybercrimes that threaten cybersecurity. It also aimed to evaluate the nature of cybersecurity and clarify the key concepts associated with it, as well as the concepts related to the types of threats and cybercrimes. The study sheds light on these threats while identifying the most important countermeasures, in addition to identifying the most prominent tools and techniques used by digital media to raise awareness about cybersecurity.

The study used a descriptive analytical approach and utilized a questionnaire to collect data from a sample of 46 media professionals in Egyptian media institutions, across the fields of journalism, radio, and television. The study achieved a number of results, the most important of which is that digital media plays a prominent role in enhancing public awareness of the risks that can threaten cybersecurity. The results also show that digital media significantly contributes to empowering the public to confront cyber threats and crimes.

[10] Al-Buhairi, Sherine. The role of digital media in enhancing cybersecurity and combating cyber threats and crimes, Scientific Journal of Public Relations and Advertising Research, 2023, (25).

6- A study by Mushawar (2023) titled 'The Role of Digital Media in Reducing Cyber Crimes - The Websites *Al-Shorouk* and *Akhbar Al-Watan* Online as a Model.'[11]

This study sought to assess the impact of digital media on cybercrime prevention efforts, as well as to highlight the key roles of local legislation and laws in Algeria and regional laws in Arab countries that address the field of combating cybercrime. The study also aimed to outline the mechanisms for using digital media to raise public awareness of the risks of cybercrime.

The study used the descriptive analytical approach and relied on content analysis of selected Algerian websites, namely Al-Shorouk and Akhbar Al-Watan. The study reached several findings, the most important of which is that digital media enhances the awareness of the Algerian public about the risks of cybercrimes through the awareness campaigns, advertisements, and educational lectures it presents. It also found that the media addresses preventive measures and individual and collective protection procedures. Finally, the study emphasized the importance of cooperation between media and government institutions to ensure a safe cyber environment.

7- The study by Al-Ku'ah and Abu Hassan (2023) titled "The Role of Arab Media and Digital Security Media in Raising Awareness Among the Public in the Arab World About Cryptocurrency Crimes."[12]

This study sought to identify the key roles played by Arab media and digital security media in enhancing Arab public awareness of crimes related to digital currencies, and it aimed to assess the extent to which the media contributes to increasing the

[11] Mushawar, Amina. (2023). The Role of Digital Media in Reducing Cyber Crimes, Doctoral Study, Ahmed Draa University, Algeria.
[12] Al-Ku'ah, Ma'in Fathi and Abu Hassan, Hala Hashem. (2023). The Role of Arab Media and Digital Security Media in Raising Public Awareness in the Arab World About Cryptocurrency Crimes, Journal of Public Relations Research, Egyptian Public Relations Association, (11) 47.

community's ability to confront these cybercrimes. The study used a sequential exploratory multi-method approach, which included collecting and analyzing quantitative data obtained through a survey applied to a sample of the Arab audience consisting of 1,305 participants, in addition to conducting a set of organized interviews with 10% of the survey participants to assess the nature of the awareness messages broadcasted through digital and security media. Twenty interviews were conducted with 20 academics and specialized experts to analyze the results and suggest interventions. The study also conducted a content analysis of ten Facebook pages that play a role in digital media.

The study reached a series of findings, the most important of which is that 64% of participants do not have information about cryptocurrency crimes. Additionally, most participants did not receive awareness messages through traditional or digital media regarding cryptocurrency crimes. The results of the study also indicate that security digital media did not provide sufficient information about the subject of cryptocurrencies or related crimes. The study highlights the necessity of enhancing social responsibility in media.

8- The study by Limna,et al. (2022). titled "The relationship between cyber security awareness, knowledge, and behavioral choice protection among mobile banking users in Thailand". [13]

This study aimed to assess the relationship between awareness of cybersecurity, knowledge, and protective behavior among users of mobile banking services in Thailand. The study employed a quantitative approach and utilized directed questionnaires with a sample that included 450 users of mobile banking services in

[13] Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The relationship between cyber security awareness, knowledge, and behavioral choice protection among mobile banking users in Thailand. International Journal of Computing Sciences Research, 6, 1-19.

Thailand.

The study concluded with results that highlighted a positive impact of knowledge and cyber awareness on protective behavior decision-making. It also emphasized the importance of training and awareness in improving personal cybersecurity.

Commentary on Literature Review

Content Commentary: Commenting on the content of previous studies:

All studies agree in their discussion of the topic of cybersecurity, as all the studies addressed the risks of cybersecurity and the best mechanisms to face these threats and mitigate them. The studies by (Al-Tamimi, 2024; Al-Qahtani et al., 2024; Al-Buhairi, 2024; Mushawar, 2023; Al-Ku'ah and Abu Al-Hassan, 2023; and Limna et al., 2022) discussed the role of digital media in raising public awareness about cybersecurity and its threats, and how to confront them. Meanwhile, the focus of the studies by (Wang et al., 2024 & Hassan et al., 2024) was on the importance of achieving cybersecurity in the banking and financial sector and the most important cybersecurity practices in this vital sector.

Commenting on the results of previous studies:

All previous studies have concluded that all institutions, especially banks and the financial sector, are suffering from numerous cyber risks and threats, as these institutions are no longer capable of facing the cyber challenges faced by various sectors. It has also been found that there is a positive relationship between the roles of digital media and the enhancement of awareness regarding cyber risks.

Benefits derived from previous studies:

Through previous studies, the researcher was able to identify the research problem, which focuses on the role of digital media in raising awareness of cybersecurity risks. This study assisted the researcher in selecting a theory where the media framing

theory was chosen to explain the roles played by digital media in the banking sector and to enhance awareness of practices to combat cyber threats. Moreover, previous studies help the researcher to establish the objectives, questions, and hypotheses related to the research topic.

Theoretical Framework

This study adopts the Framing Theory, as this theory aligns with the goals that this study aims to achieve. It focuses on interpreting the role of digital media in the banking sector in influencing the perceptions of bank employees in Bahrain, which occurs through selecting certain angles and presenting them within a specific context. The content provided by digital media in the banking sector enhances others' awareness of the impact of digital media on the thinking of employees. Studies that have used this theory confirm that visual imagery (such as YouTube clips) and other means are more effective in conveying messages to others (bank employees, both Bahrainis and non-Bahrainis). Visual imagery facilitates practitioners' efforts in raising awareness about cybersecurity risks, through the implicit messages emphasized in videos, published articles, and others.

One of the most prominent definitions provided for the media framing is "the framing of an event and making it more prominent in the media text with the use of a specific style to describe the issue or problem being presented (enhancing public awareness of cyber risks) and presenting the accompanying causes and dimensions." Additionally, one of the focal points of this theory is that through the theory, the priorities that media content seeks to achieve through what is presented are determined, highlighting the most important topics and their contribution to influencing the audience.

Justifications for choosing the theory:

One of the most prominent justifications presented by the researcher for choosing the

media framing theory in this study is as follows:

1. This theory provides an in-depth view of the media content presented across all media platforms, through a set of mechanisms and means of framing.
2. This theory plays an important role in understanding the content within the media published, which contributes to raising public awareness about cyber risks, through a set of meanings, significances, symbols, and images.
3. The framing theory plays its role in constructing a targeted media message by focusing on various practices to enhance public awareness of cyber risks and disseminating these elements according to framing tools represented in the omission and addition of metaphors, meanings, catchy phrases, metaphorical images, symbols, and connotations.
4. This theory provides an opportunity for specialists to measure the implicit content of digital media in the banking sector and its impact on the behaviors and attitudes of employees in order to enhance their awareness of cyber risks.

Cybersecurity Risk Management

The Risk Management Theory is one of the theories that can be used to identify mechanisms for dealing with the cyber security risks faced by banks. Through this theory, it is possible to analyze and evaluate the nature and level of cyber threats confronting banks, and accordingly develop a set of strategies, particularly proactive strategies, that can mitigate the negative impacts resulting from cyber security challenges in their known context. It can be said that this theory focuses on assessing potential risks in cyberspace and then adopting critical and well-considered decisions that can protect the digital assets and data of individuals and institutions (Al-Zahrani, 2024)[14].

[14] Al-Zahrani, Taghreed. (2024). The Role of Digital Media in Raising Awareness of Mental Health in Saudi Society : (A Field Study). Journal of Arts, Literature, Humanities, and Social Sciences, 2024 (99).

Al-Mutairi (2018) believes that in light of this theory, there is a set of elements through which cyber risks can be assessed and managed. Among the most prominent elements of this theory are:

1. Risk identification: This is the phase that involves identifying cyber threats that could affect systems, including malware and cyber-attacks.
2. Risk Analysis: At this stage, the likelihood of risks and their levels are assessed, which contributes to classifying risks based on their priorities.
3. Risk Treatment: This stage involves formulating the plans used to address the identified risks. Among the solutions proposed at this stage are encryption techniques and improving firewalls, and most importantly, training employees on cybersecurity.
4. Risk Monitoring: In this stage, banks continuously monitor risks to ensure that preventive measures are implemented and updated as needed.

Methodological Framework

Research Methodology:

This study used the descriptive analytical approach, which is one of the most commonly used methods in social sciences in general, and in media and security studies in particular. This approach helps researchers analyze the phenomenon under study in depth, as it seeks to interpret the factors behind the occurrence of the phenomenon. The descriptive analytical method also enables the researcher to arrive at answers to the study's questions and test the hypotheses.

The researcher used this methodology in order to reach a quantitative description of the role of digital media in enhancing awareness of cybersecurity risks in the banking sector in the Kingdom of Bahrain. It serves as a means to provide indications of the interrelation between variables, and through statistical description, the researcher can

reach results objectively, as this methodology helps avoid the interpretation of answers to questions. It also assists the researcher in making comparisons between the findings of this study and other studies on the topic (Al-Taher and Abdullah, 2024)[15].

Research Population and Sample

Research community:

The research community includes all employees in the banking sector in the Kingdom of Bahrain, and the total number of employees in all types of banks in the Kingdom of Bahrain, according to the statistics of the Central Bank of Bahrain at the end of 2023, is approximately (7,229) employees.

Research sample:

Based on the Krejcie & Morgan table for calculating sample size, the research sample for a total population of (7229) employees in the banking sector in the Kingdom of Bahrain will be (365) participants. Additionally, 35 participants from the total population will be targeted as a pilot sample to assess the validity and reliability of the questionnaire, thus the total sample will be (400) participants.

The following table illustrates the division of the sample members between exploratory and main:

Table (1) Distribution of the study sample

Percentage	Number	Type of sample
8.75%	35	exploratory sample
91.25%%	365	main sample
%100	400	Total

Table (1) showing the sample description for this study indicates that the researcher

[15] Al-Taher, Khalifa ; and Abdullah, Abdul Salam. (2024). The Importance of Studying the Subject of Scientific Research Methods and the Implications of Its Application in Student Research. Al-Qartas Journal of Humanities and Applied Sciences. (4)6.

divided the study sample into two types: the first type is the exploratory sample, which includes (35) participants, accounting for (8.75%), and the main sample, which includes (365) of the employees in the banking sector, accounting for (91.25%) of the total sample size of (400) participants.

Research Tool

This study used the survey method, which is one of the most important research methods used in the field of social sciences research. This method relies on collecting data from a sample of individuals to describe phenomena, analyze them, and infer relationships between variables. Therefore, through the survey method, sufficient data can be collected about the role of digital media in raising awareness of cybersecurity risks in the banking sector. One of the most prominent advantages of the survey method is that it helps reach the largest possible number of participants in the shortest time and with the least effort, especially when distributing questionnaires electronically. It also contributes to obtaining accurate responses that describe the phenomenon and identify strengths and weaknesses through the facts obtained via the questionnaire used to gather participants' opinions about the study variables (Kazem & Abbas, 2024)[16].

The questionnaire is considered one of the most prominent tools used when applying the survey method, and there are a number of features that make the questionnaire one of the most preferred data collection tools. Among these features are ease of preparation and implementation, as well as its contribution to saving time for researchers. It is characterized by low cost and comprehensiveness, as the questionnaire can cover a large geographical area, such as a group of countries. Among the advantages of the questionnaire is the ease of analyzing the data collected through it, as the numerical data collected can be analyzed using statistical analysis

[16] Kazem, Mohammed ; Abbas, Yasser. (2024). Factor analysis and its use in media research, Journal of Economics and Administration, 1(25).

programs and methods. Questionnaires ensure a high level of privacy for participants, as their identities are not disclosed, and the data collected is only used for scientific research purposes. Finally, one of the best outcomes that can be achieved through the application of the questionnaire is that the results it produces are generalizable (Abdulqader, 2024)[17].

The survey for this research consists of 20 items distributed as follows:

1. Demographic data: includes variables (gender - age - education level - job - years of experience)
2. Axis: The extent of awareness among banking sector employees regarding cyber security threats (including 5 items)
3. Axis: The most influential digital means in enhancing awareness of cyber security (including 5 items)
4. Axis: Challenges of digital media in enhancing awareness of cyber security (including 5 items)
5. Axis: Roles of digital media in educating banking sector employees about enhancing cyber security (including 5 items)

Psychometric Properties of the Research Instrument

1. Content Validity:

The validity of the questionnaire refers to "the extent to which the questionnaire is able to accurately measure what it is designed to measure" (Elabadla, 2024)[18]. This means that the validity of the questionnaire seeks to ensure that there is a correspondence between the research tool (the questionnaire) and the study

[17] Abdulqader, Habiteur. (2024). Constructing the Questionnaire in Social Research : Between Objective Criteria and Researcher Trends. Journal of Intellectual Dialogue, 17(2), 30-40.
[18] Elabadla, E. (2024). A proposed technique to calculate instrument reliability. Emirati Journal of Education and Literature, 2(1), 50-61.

objectives set out. The validity of the content of the questionnaire is verified by presenting the questionnaire to a group of referees (7) who hold doctoral degrees, and they were asked to comment on the appropriateness of the items for each dimension they belong to. The referees made a series of amendments and removed some items, resulting in the questionnaire appearing in its current form.

2. Reliability of the Research tool:

The reliability of the questionnaire refers to the extent to which the questionnaire accurately and consistently measures the same phenomenon under different times and circumstances, which means the extent to which similar results can be obtained if the questionnaire is reapplied under different conditions and on different samples (Elabadla, 2024). The reliability of the questionnaire is calculated using Cronbach's alpha coefficient.

Through the results of the pilot sample, which consisted of 35 participants, the researcher was able to calculate the reliability of the questionnaire. The main objective of the pilot study is to ensure the reliability of the items and dimensions, which enhances the possibility of applying the questionnaire to the main sample of the research. To determine the reliability of the questionnaire, Cronbach's alpha coefficients are relied upon, as shown in Table (2):

Table (2) Cronbach's alpha coefficient values for the dimensions of the questionnaire (n=35)

Axes	Number of Sample Members Survey	Number of Items	Cronbach's Alpha Reliability Coefficient
Axis: The extent of awareness of bank sector employees about cyber security threats	35	5	0.918
Axis: The most influential digital means in enhancing awareness of cyber security	35	5	0.906
Axis: Challenges of digital media in enhancing awareness of cyber security	35	5	0.855
Axis: Roles of digital media in educating bank sector employees about enhancing cyber security	35	5	0.891
Total Number of Questionnaire Items	25		0.892

It is evident from Table (2) regarding the Cronbach's alpha coefficients for the four axes that make up the questionnaire, which were obtained from the results of the exploratory study conducted on 35 employees in the banking sector in the Kingdom of Bahrain, that the Cronbach's alpha values indicate a high level of reliability for the questionnaire as a whole with its twenty items (89.2%). The reliability level for the items of the axis (the awareness of employees in the banking sector regarding cybersecurity threats), which consists of five items, is (91.8%), which is a high level.

As for the stability level of the five paragraphs that make up the axis of (the most influential digital media in enhancing awareness of cybersecurity), it is high and reaches (90.6%). The stability level of the five paragraphs that make up the axis of (challenges of digital media in enhancing awareness of cybersecurity) is also high, reaching (85.5%). Finally, the stability level of the paragraphs in the axis of (the roles of digital media in raising awareness among employees in the banking sector regarding enhancing cybersecurity) is high, reaching (89.1%).

It becomes clear from the high reliability coefficient of the questionnaire in light of Cronbach's alpha that the questionnaire can be applied and reapplied to the main study sample or another sample.

3. Internal consistency validity:

One of the most prominent definitions provided for the concept of internal consistency reliability is that it is "the ability of the questionnaire items to measure what they are actually intended to measure," and internal consistency reliability indicates the clarity of the questionnaire, its vocabulary, and its concepts to the individuals in the study sample" (Mohammed, 2017)[19]. The assessment of internal consistency reliability relies on the Pearson correlation coefficient.

[19] Mohammed, Dur. (2017). The most important methods, samples, and tools of scientific study. Al-Hikma Journal for Educational and Psychological Studies, (2017) 9.

International Journal of Educational Sciences and Arts (IJESA)
Vol. (4), No. (9)
IJESA
September 2025
المجلة الدولية للعلوم التربوية والآداب
الإصدار (4)، العدد (9)

Table (3) The correlation coefficient value between the score of each statement and the total score of the axis it belongs to, along with Cronbach's alpha coefficient for each statement (Items of the axis measuring the awareness of employees in the banking sector regarding cybersecurity threats). (n = 35)

Alpha Cronbach coefficient	Axis correlation	The phrases	M
.807	.713**	I understand the concept of cybersecurity and its importance in the banking sector.	1
.853	.816**	I can distinguish between types of cyber threats that may face the banking sector.	2
.812	.769**	I understand all the impacts resulting from cyber breaches on my work in the bank.	3
.890	.700**	I have the ability to recognize phishing attempts in emails or text messages received at the bank.	4
.890	.821**	I have knowledge of all the mechanisms targeting the bank's databases that try to steal client information, such as account numbers and passwords	5

Table (4) The value of the correlation coefficient between the score of each statement and the total score of the axis it belongs to, along with Cronbach's alpha coefficient for each statement (Items of the axis of the most influential digital means in enhancing cybersecurity awareness). (n = 35)

The phrase and the total sum	The phrase and the axis	The phrases	M
.791	.666**	The bank offers online training for employees to enhance their awareness of cybersecurity threats.	1
.810	.711**	The bank sends numerous awareness messages to employees via email or through banking applications to enhance their understanding of the cybersecurity threats faced by the bank.	2
.605	.588**	The bank provides specialized educational applications that help employees enhance their understanding of cyber risks and response mechanisms.	3
.833	.853**	There are channels provided by the bank that facilitate monitoring digital security updates, which contributes to increasing my awareness of cybersecurity.	4
.821	.622**	The bank provides us with awareness videos and publications through the bank's accounts to increase employees' understanding of cyber risks.	5

International Journal of Educational Sciences and Arts (IJESA)
Vol. (4), No. (9)
IJESA
September 2025
المجلة الدولية للعلوم التربوية والآداب
الإصدار (4)، العدد (9)

Table (5) The value of the correlation coefficient between the score of each statement and the total of the axis it belongs to, and the Cronbach's alpha coefficient for each statement (Items of the axis of challenges of digital media in enhancing awareness of cybersecurity). (n = 35)

The phrase and the total sum	The phrase and the axis	The phrases	M
.701	.863**	Some bank employees face difficulties in understanding the digital content that is published about cybersecurity.	1
.822	.901**	The rapid evolution of cyber threat forms is a serious challenge, as digital media content cannot keep up with these developments.	2
.806	.824**	Although digital media content can increase awareness, it may provide workers with the procedures and practical experience that are employed to protect banks from cyber threats.	3
.823	.804**	The interaction through digital media platforms is limited for some bank employees, which affects their ability to understand the messages directed at confronting cyber threats.	4
.800	.655**	Some bank employees resist the shift towards digital media in the face of cybersecurity threats.	5

Table (6) The value of the correlation coefficient between the score of each statement and the total score of the axis it belongs to, along with Cronbach's alpha for each statement (Items of the axis of the roles of digital media in raising awareness among employees in the banking sector about enhancing cybersecurity). (n = 35)

The phrase and the total sum	The phrase and the axis	The phrases	M
.809	.582**	Digital media enhances my awareness of the importance of protecting personal information and clients' banking data.	1
.830	.691**	The awareness campaigns carried out by the bank on its social media accounts contribute to improving my understanding of cybersecurity threats.	2
.882	.761**	The digital media content that includes videos and infographics enhances my understanding of the cyber threats that the bank may face.	3
.759	.787**	Digital media plays an important role in promoting safe practices for using technology in the bank.	4
.890	.816**	I recognize that the digital media materials being prepared and provided to bank employees meet their needs and enhance their awareness of the bank's cybersecurity threats.	5

The results of tables (3-4-5-6) regarding the value of the Pearson correlation coefficient between each item of the questionnaire and the total score of the relevant axis show that the level of internal consistency among each item in the four axes is high, which means that the level of consistency between each statement and the total score of the relevant axis is also high. Additionally, the Cronbach's alpha coefficients for each statement are high, being lower than the total score of the reliability of the axis as a whole. Furthermore, we find that the calculated value of (r) is higher than its tabulated value at a significance level of (0.05), which demonstrates the validity of the internal consistency of the items in each of the four axes.

Field Study Results

The researcher analyzes the results of the questionnaire collected from 347 participants out of a total of 365 targeted, which means that the response rate reached 94.5%. The statistical results were analyzed using SPSS v 27, relying on frequencies, percentages, the arithmetic mean, and relative frequency for each item.

First: Results of demographic data statistics:

Table (7) Statistical analysis results for the demographic variables of the participants. (n = 400)

The ratio	Repetition	Type of variable	The variable
%77.2	268	Male	Sex
%22.8	79	Female	
%19	66	Less than 30 years	Age
%48.7	169	From 30 to 39 years	
%25.9	90	From 40 to 49 years	
%6.4	22	50years or more	
%11.8	41	Secondary or higher diploma	Educational level
%62	215	Bachelor's	
%22.5	78	Master's	
%3.7	13	PhD	
%90.8	315	Non-supervisory position	The Job
%9.2	32	Supervisory job	

%54.2	188	Traditional	Type of bank
%45.8	159	Islamic	
%19.6	68	Less than 10 years	Years of experience
%41.8	145	From 10 to 14 years	
%32	111	From 15 to 19 years	
%6.6	23	20 years or more	
%100	347	Total	

Analysis of the statistical data of participants working in the banking sector in the Kingdom of Bahrain shows that male participants represent (77.2%), while female participants represent (22.8%). Statistics regarding age indicate that the highest percentage is among participants aged 30 to 39 years, accounting for (48.7%), and participants aged 40 to 49 years represent (25.9%). As for the participants in the age group under 30 years, they represent (19%) the total sample, and the percentage of participants in the age group of 50 years and older is 6.4%. Regarding the variable of education level, (62%) of the participants hold a bachelor's degree, and (2.5%) hold a master's degree, while those with a secondary qualification or higher diploma represent (1.8%), and those with a PhD degree represent (3.7%). Concerning the job variable, (90.8%) of the participants have non-supervisory jobs, while those with supervisory jobs represent (9.2%). Statistics show the type of bank in which participants work, with (54.2%) working in traditional banks, while (45.8%) work in Islamic banks. Analyzing the experience statistics of the participants reveals that those with 10 to 14 years of experience represent (41.8%), those with 15 to 19 years of experience represent (32%), those with less than 10 years of experience represent (19.6%), and those with 20 years or more of experience represent (6.6%).

The answer to the first study question:

The text of the first question was **(What is the extent of awareness among bank sector employees regarding cybersecurity threats?**). In order for the researcher to answer this question, she calculated the arithmetic averages and the relative importance of the responses from the study sample regarding the statements of the

axis (the extent of awareness among bank sector employees regarding cybersecurity threats).

Table (8) Sample Responses for the Axis (Awareness of Workers in the Banking Sector about Cybersecurity Threats). (N= 347)

Direction of the phrase	Relative importance	Arithmetic mean	Strongly disagree %	Disagree %	Neutral %	Agree %	Strongly agree %	
Very high	86.4%	4.32	%0.10	%2.70	%20.80	%37.40	%39.00	1- Understand the concept of cybersecurity and its importance in the banking sector.
Very high	86.6%	4.33	%5.00	%4.10	%12.30	%30.50	%48.10	2- I can identify the types of cyber threats that the banking sector may face.
Average	65.2%	3.26	%1.00	%9.20	%30.80	%30.00	%29.00	3- I understand all the effects that cyber breaches have on my work in the bank.
Very high	89%	4.45	%1.00	%2.40	%12.00	%29.60	%55.00	4- I have the ability to recognize phishing attempts in emails or text messages sent to me from the bank.
High	%71	3.55	%5.00	%5.00	%22.00	%34.00	%34.00	5- I have knowledge of all the mechanisms for targeting the bank's databases that attempt to steal customer information such as account numbers and passwords.
High	%79.6	3.98	2.42%	4.68%	19.58%	32.30%	41.02%	Total

Through the statistical description of the axis (the extent of awareness among bank sector employees regarding cybersecurity threats), the researcher finds that employees in the banking sector in the Kingdom of Bahrain possess a high level of awareness of cybersecurity threats. This is attributed to the high arithmetic mean of all items of the axis, which is (3.98) out of (5.00), and the relative importance of all items which reached (79.6%). The first statement ranked first with a mean of (4.45) and a relative importance of (89%), which confirms a very high level of agreement with the content of the statement that states, "I have the ability to recognize phishing attempts in emails or text messages received from the bank." The third statement had

the lowest mean of (3.26) and a relative importance of (62.2%), indicating a moderate level of agreement with the content of the statement that states, "I understand all the effects resulting from cyber breaches on my work in the bank."

The answer to the second study question states:

(**What are the most influential digital means in enhancing cybersecurity awareness?**). In order for the researcher to answer this question, she calculated the arithmetic averages and relative importance of the study sample's responses to the statements of the axis (the most influential digital means in enhancing cybersecurity awareness).

Table (9) Sample responses to the axis (the most influential digital means in enhancing cybersecurity awareness) (N= 347)

Direction of the phrase	Relative importance	Arithmetic mean	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	
			%	%	%	%	%	
High	%83.8	4.19	%7.60	%7.00	%3.10	%30.40	%51.90	1- The bank offers online training for employees to improve their awareness of cybersecurity threats.
High	%75.2	3.76	%5.00	%4.00	%6.00	%41.00	%44.00	2- The bank sends many awareness messages to employees via email or through banking apps to enhance their understanding of the cybersecurity threats faced by the bank.
High	%73.6	3.68	%1.20	%4.60	%18.00	%36.40	%39.80	3- The bank provides specialized educational applications that help employees enhance their understanding of cyber risks and response mechanisms.
High	%80.6	4.03	4.90%	4.70%	9.80%	44.20%	36.40%	4- There are channels provided by the bank that facilitate keeping up with digital security updates, which contributes to increasing my awareness of cybersecurity.
High	%77	3.83	2.30%	6.60%	17.50%	48.20%	25.40%	5- The bank provides us with educational videos and posts through the bank's accounts to enhance employees' understanding of cyber risks.
High	%78	3.89	4.20%	5.38%	10.88%	40.04%	39.50%	Total

Through the statistical description of the paragraphs of the axis (the most influential digital means in enhancing cybersecurity awareness), it is clear to the researcher that there is a high agreement on the use of the banking sector in the Kingdom of Bahrain for digital means that have a high impact in enhancing cybersecurity awareness. This is attributed to the high arithmetic mean of all the paragraphs of the axis, which is (3.89) out of (5.00), and the relative importance of all paragraphs, which reached (78%). The first paragraph ranked first with a mean score of (4.19) and a relative importance of (83.8%), which confirms the existence of a high level of agreement on the content of the paragraph stating that (the bank offers online training for employees to enhance their awareness of cybersecurity threats). The third paragraph had the lowest mean score of (3.68) and a relative importance of (73.6%), indicating a high level of agreement on the content of the paragraph stating that (the bank provides specialized educational applications that help employees enhance their understanding of cybersecurity risks and coping mechanisms).

Answer to the third study question:

The text of the third question is (**What are the challenges of digital media in enhancing awareness of cybersecurity in the banking sector?**). In order for the researcher to answer this question, she calculated the arithmetic averages and the relative importance of the responses of the study sample on the statements of the axis (challenges of digital media in enhancing awareness of cybersecurity in the banking sector).

Table (10) Sample Responses to the Axis (Challenges of Digital Media in Enhancing Cybersecurity Awareness in the Banking Sector) (N= 347)

Direction of the phrase	Relative importance	Arithmetic mean	Strongly disagree %	Disagree %	Neutral %	Agree %	Strongly agree %	
High	%77.8	3.89	1.40%	4.00%	18.50%	30.00%	46.10%	1- Some bank employees are facing difficulty understanding the digital content that is being published about cybersecurity.
High	%77	3.85	0.10%	3.00%	19.60%	40.20%	37.10%	2- The rapid evolution of cyber threat forms is considered a serious challenge, as digital media content cannot keep up with these developments.
Average	%67	3.35	%13.60	%2.40	%33.00	%28	%23.00	3- Although digital media content can raise awareness, it can also provide workers with the procedures and practical experience used to protect banks from cyber threats.
High	%78.2	3.91	%2.30	%1.10	%3.10	%34.00	%59.50	4- The interaction through digital media platforms is limited for some bank employees, which affects their ability to understand the messages aimed at addressing cyber threats.
High	%82	4.1	%1.00	%5.40	%12.00	%25.40	%56.20	5- Some bank employees resist the shift towards digital media in the face of cyber threats.
High	%76.4	3.82	3.68%	3.18%	17.24%	31.52%	44.38%	Total

Through the statistical description of the paragraphs of the axis (Challenges of Digital Media in Enhancing Awareness of Cybersecurity in the Banking Sector), it is clear to the researcher that there is a high agreement on the challenges faced by digital media in enhancing awareness of cybersecurity in the banking sector. This is attributed to the high arithmetic mean of all the paragraphs of the axis, which is (3.82) out of (5.00), and the relative importance of all paragraphs, which reached (76.4%). The fourth paragraph ranked first with a mean score of (4.1) and a relative importance

of (82%), which confirms a high level of agreement on the content of the paragraph stating that (some bank employees resist the shift towards digital media in the face of cyber threats). The third paragraph had the lowest mean score (3.35) and a relative importance (67%), indicating a moderate level of agreement on the content of the paragraph stating that (although digital media content can increase awareness, it may provide employees with the procedures and practical experience used to protect banks from cyber threats).

The answer to the fourth study question states:

(**What are the roles of digital media in raising awareness among workers in the banking sector to enhance cybersecurity?**). In order to answer this question, the researcher calculated the arithmetic averages and relative importance of the responses of the study sample to the statements concerning the axis (Roles of digital media in raising awareness among workers in the banking sector to enhance cybersecurity).

Table (11) Sample Responses to Theme (Roles of Digital Media in Raising Awareness of Workers in the Banking Sector about Enhancing Cybersecurity) (N= 347)

Direction of phrase	Relative importance	Arithmetic mean	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	
			%	%	%	%	%	
Very high	%84.4	4.22	%1.60	%4.00	%7.20	%33.20	%54.00	1-Digital media reinforces my awareness of the importance of protecting personal information and banking data for clients.
High	%69.4	3.47	%3.00	%14.00	%9.00	%28.00	%46.00	2- The awareness campaigns 2 carried out by the bank on its social media accounts contribute to improving my understanding of cybersecurity threats.
Average	%66.4	3.32	%1.20	%4.50	%19.30	%27.30	%47.70	3- The digital media content tha includes videos and infographics enhances my understanding of the cyber

								threats that the bank may be exposed to.
High	%79.4	3.97	%1.80	%2.80	%15.70	%30.60	%49.10	4- Digital media plays an important role in promoting safe technology practices in the bank.
High	%80	4.0	%8.30	%2.40	%13.20	%31	%45.50	5- I realized that the digital med materials prepared and presented to the bank employees meet their needs and enhance their awareness of the bank's cybersecurity threats.
High	%75.9	3.79	3.18%	5.54%	12.88%	30.02%	48.46%	Total

Through the statistical description of the paragraphs related to the axis (The roles of digital media in raising awareness among employees in the banking sector about enhancing cybersecurity), it becomes clear to the researcher that there is a high agreement on the roles played by digital media in raising awareness among employees in the banking sector about enhancing cybersecurity in the banking sector. This is attributed to the high arithmetic mean of all paragraphs of the axis, which is (3.79) out of (5.00), and the relative importance of all paragraphs, which reached (75.9%). The fourth item came in the first rank with an arithmetic average of (4.22) and a relative importance of (84.4%), which confirms a high level of agreement on the content of the item stating that (digital media enhances my awareness of the importance of protecting personal information and customers' banking data). The third item, on the other hand, had the lowest arithmetic average (3.32) and a relative importance of (66.4%), indicating a moderate level of agreement on the content of the item stating that (digital media content that includes videos and infographics enhances my understanding of the cyber threats that the bank may face).

Testing the hypotheses (Answers to questions five and six):

To test the first hypothesis which states (There is a statistically significant relationship between the digital media used in banks and the level of awareness of

employees in countering cyber-attacks), the researcher conducts a simple linear regression test between the total score of the items in the axis (digital media used in banks) and the total score of the items in the axis (roles of digital media in raising awareness of employees in the banking sector about enhancing cybersecurity) as shown in Table No. (12)

Table (12) Results of the analysis of variance for multiple regression to test the effect size of the overall degree of digital media used in banks and the level of awareness of employees in countering cyber-attacks.

Level of significance Sig	Value of the test F	Determination coefficient R2	Correlation coefficient R	Mean Squared	Degrees of freedom	Sum of squares	Source of variation
0.000	56.11	0.263	.513[a]	22.781	1	22.781	The decline
				.406	346	63.741	The leftovers
					347	86.522	Total

It is clear to the researcher from the outputs of the multiple regression analysis for testing the effect size of the overall score of digital media used in banks and the awareness level of employees in confronting cyber-attacks that (there is a statistically significant relationship between the digital media used in banks and the awareness level of employees in confronting cyber-attacks). This is interpreted in light of the high calculated F test value (56.111). The relationship between the two variables emerges as a result of the observed significance level being (0.000), which is less than the standard significance level (0.01 - 0.05). The significance of the effect is also more clearly shown through the value of the correlation coefficient R, which is (0.513), indicating that (the digital media used in banks) is responsible for 51.3% of any increase or decrease in (the awareness level of employees in confronting cyber-attacks). As for the value of the R2 coefficient, it is (0.263), which indicates the strength of the relationship between the independent variable (the digital media used in banks) and the dependent variable (the level of awareness of employees in combating cyber-attacks), amounting to 26.3%. Based on these values and their interpretation mechanisms, the first main hypothesis is accepted, and the null

hypothesis is rejected. Hence, the researcher concludes that (**there is a statistically significant relationship between the digital media used in banks and the level of awareness of employees in combating cyber-attacks**).

To test the second hypothesis which states that "there are statistically significant differences between the opinions of employees in the banking sector regarding the role of digital media in enhancing awareness of cybersecurity threats, attributed to variables (gender - age - job - type of bank)," the researcher applies the T-Test for statistical significance between male and female participants. To verify the significance of differences between the variables (age - job - type of bank), the researcher calculates the average responses of the research sample individuals regarding the opinions of employees in the banking sector on the role of digital media in enhancing awareness of cybersecurity threats. An Analysis of Variance (ANOVA) test was also conducted to determine the significance of the differences between the average responses of the study population.

Table (13) Averages and standard deviations and the statistical significance test for the T-Test differences between male and female participants regarding the opinions of employees in the banking sector on the role of digital media in enhancing awareness of cybersecurity threats attributed to the variable of gender (N=347)

The indication	Value the indication	Value (t)	79 = Female		268 = Male		Variables
			Sd.	M	Sd.	M	
Insignificant	.502	.707	.755	3.67	.595	3.66	The role of digital media in enhancing awareness of cybersecurity threats.

The values presented in Table No. (13), which discusses the means, standard deviations, and significance testing (T-Test) for the differences between male and female participants regarding the opinions of employees in the banking sector about the role of digital media in raising awareness of cybersecurity threats, indicate that the differences attributed to the gender variable are not statistically significant (sig = 0.502 at (0.01) or (0.05)). This implies that there is a consensus between the opinions of both males and females regarding the role of digital media in raising awareness of

cybersecurity threats, meaning that there are no statistically significant differences between the opinions of employees in the banking sector about the role of digital media in enhancing awareness of cybersecurity threats attributable to the gender variable. To verify the significance of the differences between the age category variable (under 30 years - from 30 to 39 years - from 40 to 49 years - 50 years and above), the researcher calculated the averages of the responses from the sample participants regarding the role of digital media in enhancing awareness of cybersecurity threats. An analysis of variance (ANOVA) test was also conducted to determine the significance of the differences between the average responses of the study population.

Table (14) Analysis of variance ANOVA regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to the variable of age (N=347)

The overall degree of the role of digital media in enhancing awareness of cybersecurity threats is attributed to the age variable.	Descriptive statistics	Number	Age
3.68	Arithmetic mean	66	Less than 30 years
0.63	Standard deviation		
3.59	Arithmetic mean	169	From 30 to 39 years
0.81	Standard deviation		
3.99	Arithmetic mean	90	From 40 to 49 years
0.89	Standard deviation		
3.74	Arithmetic mean	22	50 years or more
0.69	Standard deviation		
1.742	Value of F	Results of the analysis of variance	
0.318	Value of the indication		
Insignificant	Level of significance		

The values presented in Table No. (14), which discusses the averages, standard deviations, and significance testing (T-Test) for the differences between participants from various age groups regarding the opinions of employees in the banking sector about the role of digital media in enhancing awareness of cybersecurity threats, indicate that the differences are statistically insignificant (sig=0.318) at (0.01) or (0.05). This suggests that there is a convergence of opinions among all age groups

regarding the role of digital media in enhancing awareness of cybersecurity threats, meaning that there are no statistically significant differences in the views of banking sector employees about the role of digital media in enhancing awareness of cybersecurity threats attributed to the age variable.

Table (15) Analysis of variance ANOVA regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to the variable of occupation. (N=347)

The overall degree of the role of digital media in enhancing awareness of cybersecurity threats is attributed to the variable of function.	Descriptive statistics	Number	The Job
3.66	Arithmetic mean	315	Non-supervisory jobs
.68	Standard deviation		
3.82	Arithmetic mean	315	Supervisory jobs
.84	Standard deviation		
1.992	Value of F	Results of the analysis of variance	
0.233	Value of the indication		
Insignificant	Level of significance		

The values presented in Table (15), which discusses the averages, standard deviations, and statistical significance testing (T-Test) of the differences among participants from various job functions regarding the opinions of bank sector employees about the role of digital media in enhancing awareness of cybersecurity threats, indicate that the differences are not statistically significant (sig=0.233 at 0.01 or 0.05) in the role of digital media in enhancing awareness of cybersecurity threats. This suggests that there is a convergence in the opinions of all participants from different types of jobs (non-supervisory and supervisory) regarding the role of digital media in enhancing awareness of cybersecurity threats, meaning that there are no statistically significant differences between the opinions of bank sector employees about the role of digital media in enhancing awareness of cybersecurity threats attributed to job function.

Table (16) Analysis of variance ANOVA regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to the variable of bank type. (N=347)

The overall degree of the role of digital media in enhancing awareness of cybersecurity threats is attributed to the variable type of bank.	Descriptive statistics	Number	Type of bank
3.60	Arithmetic mean	188	بنوك تقليدية
.66	Standard deviation		
3.79	Arithmetic mean	188	بنوك اسلامية
.79	Standard deviation		
1.628	Value of F	Results of the analysis of variance	
0.447	Value of the indication		
Insignificant	Level of significance		

The values shown in Table 16, which discusses the means and standard deviations and the statistical significance test (T-Test) of the differences between participants from various job roles regarding the opinions of bank sector employees on the role of digital media in enhancing awareness of cybersecurity threats, are attributed to the variable of bank type. The differences are statistically insignificant (sig=0.447 at (0.01) or (0.05)) regarding the role of digital media in enhancing awareness of cybersecurity threats. This indicates that there is a convergence among the opinions of all participants from different types of banks (traditional and Islamic) regarding the role of digital media in enhancing awareness of cybersecurity threats, meaning that there are no statistically significant differences between the opinions of bank sector employees on the role of digital media in enhancing awareness of cybersecurity threats attributed to the variable of bank type.

In summary, the researcher concludes that the second hypothesis is not accepted, meaning that) there **are no statistically significant differences between the views of employees in the banking sector regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to the variables of 'gender, age, job, and type of bank'**).

Conclusions

drawn after presenting and discussing the results in light of a set of questions that achieve the study's objectives are as follows:

1. Employees in the banking sector in the Kingdom of Bahrain have a high level of awareness of the threats of cybersecurity that can impede the services provided by banks and pose a risk to the confidentiality of customer data and their banking transactions. The employees understand the concept and importance of cybersecurity in this vital sector.
2. Banks in the Kingdom of Bahrain rely on a variety of digital tools that help enhance employees' awareness of cybersecurity and its threats. These tools include online platforms that provide training for employees, social media accounts belonging to the banks which are used to send updates to employees regarding cybersecurity threats, and awareness messages that are sent via email to employees.
3. The processes of raising awareness among bank employees about cybersecurity threats face a number of challenges, the most important of which is resistance to change; some employees do not accept digital transformation and the changes associated with media. Additionally, some employees struggle to understand the digital content published about cybersecurity. There is also the inability of digital media to keep up with the rapid changes in the field of cybersecurity threats.
4. Digital media, through its various means, plays important roles in educating employees in the banking sector about enhancing cybersecurity. Among the most prominent of these roles is raising the awareness of banking sector employees about the importance of protecting personal information and customer banking data, tailoring the digital media materials prepared and presented to employees to their needs, and enhancing their awareness of the bank's cybersecurity threats.

Digital media also plays a central role in disseminating safe practices for using technology in the bank.

5. There is a statistically significant relationship between the digital media used in banks and the level of awareness among employees in combating cyber-attacks, as the more effective the digital media used in the banking sector, the more capable these media are of increasing employees' awareness of cybersecurity threats and guiding them to deal with them efficiently and effectively.
6. There are no statistically significant differences in the opinions of employees in the banking sector regarding the role of digital media in enhancing awareness of cybersecurity threats attributed to variables (gender - age - job - type of bank).

Recommendations

1. I recommend the banking sector in the Kingdom of Bahrain to utilize digital media more effectively in order to simplify the digital content being published about cybersecurity and make it more engaging and exciting.
2. I recommend those responsible for digital media in the banking sector to focus on keeping up with the technological developments occurring in the field of cybersecurity and to provide continuous content for employees regarding these technological changes and the endless threats.
3. I recommend employees in the banking sector in the Kingdom of Bahrain to interact with the digital content being published about the cybersecurity threats facing banks and to inquire from specialists about the nature of the threats that are difficult to understand.
4. I recommend cybersecurity specialists in the banking sector to explain all the impacts resulting from cyber breaches on my work field in the bank through what is published to employees as digital content.

5. I recommend conducting future studies on the role of digital media in training employees to reduce the level of cybersecurity threats in the public sector in the Kingdom of Bahrain.

References

1. Abdulqader, Habiteur. (2024). Constructing the Questionnaire in Social Research: Between Objective Criteria and Researcher Trends. Journal of Intellectual Dialogue, 17(2), 30-40.
2. Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research*, *37*(4), 17-32.
3. Al-Buhairi, Sherine. The role of digital media in enhancing cybersecurity and combating cyber threats and crimes, Scientific Journal of Public Relations and Advertising Research, 2023, (25).
4. Al-Ku'ah, Ma'in Fathi and Abu Hassan, Hala Hashem. (2023). The Role of Arab Media and Digital Security Media in Raising Public Awareness in the Arab World About Cryptocurrency Crimes, Journal of Public Relations Research, Egyptian Public Relations Association, (11) 47.
5. Al-Omari, Hamad. (2022). Management of Cyber Crises and Their Impact on Bahraini National Security: A Practical Study in Light of the Cybersecurity Strategy of the Kingdom of Bahrain, master's Thesis, Royal Police Academy, Kingdom of Bahrain.
6. Al-Qahtani, Al-Lulu, Al-Mutairi, Shaqra Muhammad, and Al-Juhani, Amani Saleh. (2024). The role of Saudi digital media in raising citizens' awareness about cybercrime techniques in the Kingdom of Saudi Arabia (Field Study), Journal of Arts, Literature, Humanities and Social Sciences, 2024 (104).
7. Al-Taher, Khalifa; and Abdullah, Abdul Salam. (2024). The Importance of Studying the Subject of Scientific Research Methods and the Implications of Its Application in Student Research. Al-Qartas Journal of Humanities and Applied Sciences. (4)6.
8. Al-Tamimi, Abdulaziz. (2024). The Role of Digital Media in Raising Awareness of the Risks of Cyber Crimes, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia.

9. Al-Zahrani, Taghreed. (2024). The Role of Digital Media in Raising Awareness of Mental Health in Saudi Society: (A Field Study). Journal of Arts, Literature, Humanities, and Social Sciences, 2024 (99).
10. Elabadla, E. (2024). A proposed technique to calculate instrument reliability. *Emirati Journal of Education and Literature*, *2*(1), 50-61.
11. Fact Sheet | CBB. (2024). Retrieved from www.cbb.gov.bh website:

https://www.cbb.gov.bh/fact-sheet/

12. Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.
13. Hossam, Mansour. (2022). Digital Media: Its Concept, Means, Theories, Journal of Research and Studies in New Media, (3)2.
14. Kazem, Mohammed; Abbas, Yasser. (2024). Factor analysis and its use in media research, Journal of Economics and Administration, 1(25).
15. Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The relationship between cyber security awareness, knowledge, and behavioral choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, *6*, 1-19.
16. Mohammed, Dur. (2017). The most important methods, samples, and tools of scientific study. Al-Hikma Journal for Educational and Psychological Studies, (2017) 9.
17. Mushawar, Amina. (2023). The Role of Digital Media in Reducing Cyber Crimes, Doctoral Study, Ahmed Draa University, Algeria.
18. Qouich, Jamal al-Din, (2017) Media Education and Digital Media: A Study on Challenges and Strategies, Al-Risala Journal for Human Studies and Research, (2)3.
19. Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, *147*, 104051.