ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (42-52), Month: October - December 2023, Available at: www.researchpublish.com

The Impact of Using ChatGPT on Cybersecurity & Social Engineering

[1]Dr. Khaled Khalifah Allanqawi, [2]MOHAMMAD HUSSEIN ALSAIDOMAR

Higher Institute of Energy

The Public Authority for Applied Education and Training, Kuwait

DOI: https://doi.org/10.5281/zenodo.10142464

Published Date: 16-November-2023

Abstract: **ChatGPT has emerged as a noteworthy avenue within the realm of artificial intelligence (AI). In the contemporary digital landscape, the predominant focus of research endeavors revolves around the multifaceted implications of this technology. While numerous scholars, particularly those with expertise in programming and digital security, have acknowledged the existence of a correlation between ChatGPT and cybersecurity as well as social engineering, a comprehensive exploration of this relationship remains conspicuously absent from the academic discourse. The objective of this scholarly work is to elucidate the ramifications of ChatGPT on the domains of cybersecurity and social engineering. To accomplish this aim, a descriptive-analytical approach has been employed to meticulously dissect and assess the influence of ChatGPT. This analysis is conducted from the perspectives of information technology specialists, ChatGPT experts, and cybersecurity professionals operating within the geographical purview encompassing the United Arab Emirates, the Kingdom of Saudi Arabia, the State of Kuwait, and the Arab Republic of Egypt. The research cohort consists of a substantial sample size comprising 93 such professionals, and data collection is facilitated through the utilization of a structured questionnaire. Subsequently, the amassed dataset is subjected to rigorous statistical analysis employing the SPSS statistical software version 22. The findings of this investigation substantiate the presence of a statistically significant impact emanating from ChatGPT on the practices of cybersecurity and the occurrence of social engineering attacks.**

Keywords: **Artificial intelligence – ChatGPT – Cybersecurity – Social engineering.**

1. INTRODUCTION

The late 20th and early 21st centuries witnessed rapid advancements in telecommunications, computing hardware and software, and data encryption. These technological developments laid the foundation for significant transformations in the 21st century, particularly in the domains of electronic data processing, artificial intelligence (AI), and machine learning. Consequently, AI and machine learning have assumed pivotal roles in the contemporary landscape, reshaping the landscape of scientific inquiry. Notably, the evolution of AI has engendered novel perspectives and paradigms across various industries, with a profound impact on natural language processing being particularly noteworthy. Among the noteworthy developments in this sphere is the advent of conversational agents, colloquially referred to as chatbots. These sophisticated computer programs are purposefully designed to engage in dialogues with individuals through messaging platforms, representing a seminal shift in human-computer interaction (Sebastian, 2023; Gill & Kaur, 2023; Ray, 2023).

Objectives of the study

The utilization of ChatGPT by cybercriminals presents a tangible threat in the context of social engineering attacks, thereby establishing a critical nexus between ChatGPT, cybersecurity, and social engineering. To illustrate, malicious actors may harness ChatGPT's capabilities to fabricate persuasive personas, initiate dialogues with targeted individuals, gain their trust, and ultimately coax them into revealing sensitive information or executing actions that compromise security measures. Conversely, cybersecurity experts can employ ChatGPT as a tool to detect and thwart social engineering endeavors.

ChatGPT's analytical prowess can empower security teams to bolster their defenses against such nefarious tactics by scrutinizing conversations and identifying indicators of social engineering attempts.

Hence, the principal objective of the present study is to elucidate the ramifications of ChatGPT on the realms of cybersecurity and social engineering. This investigation seeks to quantify the impact of ChatGPT by examining its multifaceted dimensions, encompassing both legitimate and illicit applications, on cybersecurity and social engineering within the Arab countries.

1.1 Emergence of ChatGPT

In late November 2022, Open Artificial Intelligence (AI) introduced an innovative chatbot tool by the name of ChatGPT. This remarkable tool is built upon the foundation of the Generative Pre-trained Transformer (GPT) architecture, as substantiated by the works of Haleem, Javaid, and Singh (2022) and O'Rourke (2023). Notably, ChatGPT is underpinned by the GPT-4 architecture, an advanced iteration within the GPT series, distinguished by its increased parameter count and enhanced training methodologies. Consequently, it excels in generating text that closely resembles human speech, as elucidated by Wilson (2023).

ChatGPT exhibits exceptional versatility, proficiently responding to inquiries presented in a diverse array of languages and formats, delivering responses that emulate human-like conversation. This proficiency stems from its training on an extensive dataset of conversational text, as corroborated by the works of Addington (2023), Ray (2023), Mijwil, Aljanabi, and Hussein (2023), Deng, and Lin (2022), Fitria (2023), and Dave, Athaluri, and Singh (2023).

Due to its capacity to comprehend and produce content with a human-like quality, ChatGPT has found utility across a wide spectrum of applications. These encompass but are not limited to natural language processing, text summarization, language translation, and conversation generation, as delineated by Mijwil, Aljanabi, and Ali (2023) and recognized by the Council of the European Union (2023).

1.2 Cybersecurity Practices

The advent of AI-driven applications has ushered in a plethora of opportunities, notably within domains like cybersecurity, as highlighted by Bahrini et al. (2023). In the contemporary era, safeguarding the digital landscape has emerged as an imperative concern, thereby necessitating the introduction of the cybersecurity paradigm. Cybersecurity, as elucidated by Mijwil et al. (2023), Sadiku, Fagbohungbe, and Musa (2020), Wilson (2023), Morovat and Panda (2020), and Aldawood and Skinner (2019), encompasses the multifaceted process of thwarting cyberattacks, averting damage, and preventing unauthorized access to internet-connected systems, encompassing hardware, software, and data assets.

Within the scholarly discourse, cybersecurity is conceptualized along five distinct dimensions. These dimensions encompass cybersecurity policy and strategy, cyberculture and societal aspects, cybersecurity education, training, and skills, the formulation of legal and regulatory frameworks, and the establishment of standards, organizations, and technologies. This comprehensive characterization of cybersecurity is supported by The World Bank Group (2019) and The Global Cyber Security Capacity Centre (2023).

Given the pervasive utilization of ChatGPT, concerns have arisen regarding its potential ramifications on security, as underscored by Ananthachari and Singh (2023). Cybercriminals have employed a plethora of tactics to undermine cybersecurity, making it a paramount issue anticipated to persist over the next two decades, as posited by Hove (2020) and Al-Wahaibi (2022).

1.3 Social Engineering

Social engineering constitutes a category of cyberattacks within the realm of cybersecurity, wherein threat actors exploit interpersonal interactions to capitalize on human susceptibilities, thereby compromising security protocols (Wang, Sun & Zhu, 2020; Alharthi & Regan, 2021). What distinguishes social engineering-based cyberattacks is their inherent elusiveness, as they eschew predefined patterns or conventional attack methodologies, as noted by Siddiqi, Pak & Siddiqi (2022).

Among the most innovative means of illicitly accessing information systems, social engineering stands out prominently, as highlighted by Maraj & Butler (2022), Aldawood, Alashoor & Skinner (2020), Klimburg-Witjes & Wentland (2021), and Alharthi & Regan (2021). Social engineering endeavors are characterized by their objective to coax victims into divulging sensitive information or engaging in actions that breach the protective security barriers guarding information-related assets,

thereby advancing the attacker's nefarious objectives (Fan, Lwakatare & Rong, 2017; Borkovich & Skovira, 2019; Snyder, 2015).

This methodological approach poses a substantial security hazard to the digital infrastructure, user base, data repositories, and operational processes, all in the pursuit of malicious intentions (Wang et al., 2021; Wang, Sun & Zhu, 2020; Breda, Barbosa & Morais, 2017). Social engineers employ an array of stratagems, such as phishing, to deceive users into granting access to diverse systems or revealing their personal information, as documented by Alsulami et al. (2021).

1.4 The relationship between ChatGPT, cybersecurity practices, and social engineering

The proliferation of ChatGPT in various applications necessitates a thorough consideration of both its potential advantages and drawbacks. While ChatGPT exhibits the capability to expedite and accurately disseminate information to customers or automate business operations, it concurrently raises pertinent concerns regarding its potential misuse as a hacking tool. Individuals and organizations must, therefore, diligently implement necessary security measures to safeguard against ChatGPT-related cybercrimes and social engineering exploits, as underscored by Dash & Sharma (2023).

In the event of a cyberattack, ChatGPT can prove instrumental in early detection, effective response, and enhancing internal communication, as noted by Haleem et al. (2022). Moreover, ChatGPT has introduced novel prospects in the realms of data analysis and cybersecurity, enabling information technology specialists to identify threats with greater speed and efficiency, as elucidated by Kalla & Smith (2023).

It is imperative to acknowledge that transformer-based large language models (LLMs) like the latest iteration of ChatGPT have precipitated various concerns in recent years. These concerns encompass the dissemination of false information, phishing attempts, issues of intolerance, and the emergence of new AI-based attacks, as discussed by McKee & Noever (2023), Alsulami et al. (2021), Fraiwan & Khasawneh (2023), Oche (2019), Gill & Kaur (2023), and Chakraborty, Biswas & Khan (2022).

Recent studies have accentuated the tactics employed by malicious actors who leverage social engineering to compromise an organization's security architecture. This approach capitalizes on the human element, which is often more susceptible to manipulation than identifying vulnerabilities in security systems, as highlighted by Siddiqi et al. (2022) and Rahman & Watanobe (2023). It is essential to underscore that ChatGPT operates on an extensive dataset, rendering it relatively easy for a hacker to solicit and acquire critical information. This includes details such as the number of employees within an organization and the annual salary of specific individuals, particularly as ChatGPT accumulates more interactions with users, given the absence of an external server where personal information is stored, as emphasized by Ananthachari & Singh (2023), Bahrini et al. (2023), and the Council of the European Union (2023).

1.5 Scope of the Research

In recent years, the Middle East and North Africa (MENA) region, particularly Gulf nations such as the United Arab Emirates (UAE), the Kingdom of Saudi Arabia, and Qatar, have witnessed a significant surge in the utilization of AI chatbots. This escalation can be attributed to the region's pronounced smartphone adoption rates and a populace that exhibits technological adeptness. Consequently, the MENA region has emerged as a fertile ground for the deployment of AI language models and AI-powered chatbots, including ChatGPT.

The utilization of these AI technologies holds promise and potential for various applications. They can assist in a multitude of ways, ranging from enhancing customer service and automating business processes to streamlining communication and providing information efficiently. Nevertheless, alongside these opportunities, there is a growing concern regarding the potential negative implications associated with the use of such chatbots, particularly in the context of social engineering attacks.

The adoption of AI chatbots in the MENA region presents a dual-edged sword, offering considerable benefits while concurrently necessitating vigilance and robust security measures to mitigate the risks of social engineering exploits.

1.6 Statement of the Problem

Indeed, there have been notable studies delving into the intricate relationship between ChatGPT, social engineering, and cybersecurity, as evidenced by the works of Grbic & Dujlovic (2023) and Ananthachari & Singh (2023). It's worth emphasizing that the domains of artificial intelligence, cybersecurity, and social engineering are burgeoning areas of

research that warrant further exploration, especially within the Arab region, as articulated by Shaer et al. (2023).

Given the earnest efforts exerted by Arab governments to cultivate secure digital environments for their constituents and their eagerness to harness recent advancements in the field of AI to counter social engineering attacks, it is plausible to assume that ChatGPT will indeed wield a statistically significant impact on the domains of cybersecurity and social engineering. This hypothesis underscores the pressing need to investigate and better understand the multifaceted consequences of ChatGPT deployment in the context of Arab nations.

2. MATERIAL AND METHODS

The analytical descriptive approach was selected as the most appropriate research methodology for this study, aligning with the study's inherent characteristics and objectives. The study population encompassed professionals with expertise in information technology, ChatGPT, and cybersecurity, actively engaged in their respective roles within the United Arab Emirates, the Kingdom of Saudi Arabia, Kuwait, and Egypt. The survey instrument was administered electronically, facilitated through the Google Drive application, and subsequently distributed to the study's targeted participants via email. The study sample comprised a total of 93 specialists who willingly participated in the research endeavor. The frequencies and percentages were calculated for the study sample characteristics, and they are represented in the basic data that includes:

Table (1) sample distribution according to their characteristics

Gender	**Frequency**	**Percentage**
Male	61	67.0%
Female	30	33.0%
Total	91	100.0%
Job position	**Frequency**	**Percentage**
IT specialist	33	36.3%
ChatGPT specialist	29	31.9%
Cybersecurity specialist	29	31.9%
Total	91	100.0%
Years of experience	**Frequency**	**Percentage**
Less than 5 years	27	29.7%
From 5 to less than 10 years	29	31.9%
10 years and above	35	38.5%
Total	91	100.0%
ChatGPT knowledge	**Frequency**	**Percentage**
Low	17	18.7%
Moderate	43	47.3%
High	31	34.1%
Total	91	100.0%
Country	**Frequency**	**Percentage**
Kingdom of Saudi Arabia	23	25.3%
United Arab Emirates	22	24.2%
Egypt	19	20.9%
Kuwait	27	29.7%
Total	91	100.0%

The preceding table reveals several key findings regarding the study sample:

1. Gender Distribution: A significant majority of the participants in the study were male, comprising 67.0% of the total sample.

2. Job Titles: Among the study participants, the most common job title was related to information technology (IT) specialists, accounting for 36.3% of the sample.

3. Professional Experience: A substantial portion of the study sample reported having 10 or more years of professional experience, constituting 38.5% of the participants.

4. Familiarity with ChatGPT: The majority of respondents indicated a moderate level of familiarity with ChatGPT, with 47.3% falling into this category.

5. Geographic Distribution: The largest proportion of the sample hailed from the Kingdom of Saudi Arabia, representing 25.3% of the participants.

These findings provide valuable insights into the demographic and professional characteristics of the study sample, which can inform the subsequent analysis and interpretation of research results.

Study Instrument

The researcher employed a questionnaire as the primary instrument for data collection in this study. The questionnaire underwent rigorous testing to ensure its validity and reliability.

1. Validity Testing: To assess the validity of the questionnaire, it was subjected to a review process involving multiple experts who evaluated its linguistic formulation and clarity. An impressive 80% consensus was achieved among these reviewers, indicating a strong agreement on the questionnaire's validity.

2. Internal Consistency Validity: The internal consistency of the questionnaire was assessed by calculating the Pearson correlation coefficient between the scores of each statement and the total score of the corresponding axis. Importantly, all correlation coefficients were found to be statistically significant at the 0.01 significance level, further affirming the questionnaire's internal consistency.

3. Structural Validity: The structural validity of the questionnaire's axes was confirmed by computing the correlation coefficients between each axis and the total score of the questionnaire. These coefficients exhibited high values, ranging from .937 to .993, all of which were statistically significant at the 0.01 significance level. This outcome underscores the robust structural validity of the questionnaire.

4. Reliability Assessment: Cronbach's alpha coefficients were calculated for each of the questionnaire's axes. The results revealed that the coefficients ranged from .903 to .978, with an overall value of .965. These high Cronbach's alpha values underscore the reliability of the questionnaire and its ability to yield consistent and dependable results.

In summary, the rigorous testing conducted on the questionnaire demonstrated both its validity and reliability, lending confidence to the data collected through this instrument for the purposes of the study.

Data analysis procedures

- The data analysis in this study was conducted using the Statistical Package for the Social Sciences (SPSS). Various statistical methods were employed to draw conclusions from the data, as outlined below:

- 1. Frequencies and Percentages: Frequencies and percentages were computed to characterize the research sample based on demographic data. This descriptive statistics approach provided insights into the composition of the study sample.

- 2. Arithmetic Means and Standard Deviations: Arithmetic means and standard deviations were calculated to determine the average responses to the questionnaire statements and the total scores of the questionnaire axes. This statistical analysis helped summarize the responses of the research sample and provided a measure of central tendency and dispersion.

- 3. Pearson Correlation Coefficient: The Pearson correlation coefficient was utilized to assess the internal consistency of the questionnaire. This analysis examined the relationships between individual questionnaire statements and the total scores of the corresponding axes.

- 4. Cronbach's Alpha Coefficient: Cronbach's alpha coefficient was employed to assess the reliability of the questionnaire statements. This statistic measures the internal consistency and reliability of the items within the questionnaire.

- 5. Simple Linear Regression Analysis: Simple linear regression analysis was used to test and validate the study hypotheses. This statistical method allowed the researcher to examine the relationships between variables and assess whether they influenced one another.

- By employing these statistical methods, the study was able to systematically analyze the data, draw meaningful conclusions, and test the hypotheses outlined in the research.

- **Range equation:** to determine the arithmetic mean of the responses to each statement, as follows:

The response score was determined, so that the very low degree was represented by (1), low by (2), medium by (3), high by (4), and very high by (5), while the verification degree for each axis was determined as follows:

$$\text{Category length} = \frac{\text{highest limit-lowest limit}}{\text{level No.}} = \frac{5-1}{5} = 0.08$$

- From 1 to less than 1.80 represents a (very low) response degree.
- From 1.80 to less than 2.60 represents a (low) response degree.
- From 2.60 to less than 3.40 represents a (medium) response degree.
- From 3.40 to less than 4.20 represents a (high) response degree.
- From 4.20 to less than 5 represents a (very high) response degree.

Theory

The theory of artificial intelligence first emerged in the early 1960s, marking the inception of a field that focuses on replicating human thought processes and translating these processes into technical systems (Inozemtsev, Ivleva & Ivlev, 2017). While substantial progress has been made in the theoretical foundations of artificial intelligence, a critical research gap exists in the need to explore its diverse applications (Pietikäinen & Silvén, 2021).

This research paper endeavors to address this gap by delving into the practical applications of artificial intelligence, particularly within the domains of cybersecurity and social engineering. By examining the potential utilization of this technology in these critical areas, the study aims to contribute to a comprehensive understanding of how artificial intelligence can be harnessed to enhance security measures and counter social engineering threats.

3. RESULTS

The results of the research paper will be discussed by reviewing the descriptive statistics of the study variables, and then verifying the validity of the research hypotheses as follows:

3.1 Results of the descriptive statistics of the study variables

3.1.1 Reviewing the descriptive results of the first variable "The potential uses of ChatGPT in Arab Countries"

Frequencies, percentages, means and standard deviations were calculated for the first axis: potential uses of ChatGPT dimension, and then ranked in a descending order according to each dimension's mean:

Table No. (2) Frequencies, percentages, means, and standard deviations of the participants' responses to the dimensions of the first axis: Potential uses of ChatGPT

No.	Dimensions	Mean	SD	Response degree	Rank
1	The First Dimension: Legal Uses	2.64	.526	medium	2
2	The Second Dimension: Illegal Uses	2.70	.531	medium	1
Total		2.67	.475	Medium	

Table No. (2) indicated that the first axis, which pertained to the potential use of ChatGPT, received a "medium" response degree with a mean of (2.67) according to the range equation and a standard deviation of (.475). ChatGPT is a modern and advanced form of artificial intelligence that can simulate human thinking and engage in natural conversations with responses that closely resemble those of humans. The modernity of this technology may be the reason for not obtaining a high response rate, the participants are not fully acquainted with its legal and illegal uses.

3.1.2 Reviewing the descriptive results of the second variable "Cybersecurity practices in Arab Countries"

Frequencies, percentages, means and standard deviations were calculated for the second axis: cybersecurity, and then ranked in a descending order according to each dimension's mean:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (42-52), Month: October - December 2023, Available at: www.researchpublish.com

Table No. (3) Frequencies, percentages, means, and standard deviations of the participants' responses to the dimensions of the second axis: Cybersecurity Practices

No.	Dimensions	Mean	SD	Response degree	Rank
1	The First Dimension: Policy and Strategy	2.76	.511	Medium	2
2	The Second Dimension: Culture and Society	2.71	.494	Medium	5
3	The Third Dimension: Education, Training, and Skills	2.73	.466	Medium	4
4	The Fourth Dimension: Legal and Regulatory Frameworks	2.75	.570	Medium	3
5	The Fifth Dimension: Standards, Business Models, and Technologies	2.79	.518	Medium	1
Total		2.75	.411	Medium	

As seen in Table No. (3), the mean of the second axis (Cybersecurity) response degree was (medium), with a mean of (2.75) according to the range equation, and a standard deviation (.411). This can be explained by the fact that despite relying upon artificial intelligence techniques to achieve many tasks, illegal use may pose a threat to cyber security. Thus, strict standards and regulatory frameworks should be relied upon in the process of updating and organizing software, in addition to the importance of deterrent penalties for those who commit electronic crimes.

3.1.3 Reviewing the descriptive results of the third variable "The main techniques used in social engineering attacks in Arab Countries?"

Frequencies, percentages, means and standard deviations were calculated for the third axis: social engineering techniques, and then ranked the dimensions in descending way according to each dimension's mean as follows:

Table No. (4) Frequencies, percentages, means, and standard deviations of the participants' responses to the dimensions of the third axis: social engineering techniques

No.	Dimensions	Mean	SD	Response degree	Rank
1	The First Dimension: Persuasion	2.71	.577	medium	2
2	The Second Dimension: Fabrication	2.69	.540	medium	3
3	The Third Dimension: Data gathering	2.76	.513	medium	1
Total		2.72	.468	medium	

As illustrated in Table No. (4), the mean for the third axis, which pertains to the response degree regarding social engineering techniques, was determined to be at a "medium" level, with an average score of (2.72), as computed using the range equation. The standard deviation for this axis was calculated to be approximately (.468).

This observation can be elucidated by recognizing the presence of numerous techniques employed by malicious actors in the realm of data hacking and criminal activities, all of which are illicit in nature. However, it's worth noting that these types of cyberattacks are not prevalent in Arab countries to such an extent that they pose a significant threat to the security of online communities and the safety of digital transactions.

3.2 Verifying the validity of the research hypotheses

The two hypotheses of the research will be verified using linear regression analysis as follows:

3.2.1 Verifying the first hypothesis: There is a statistically significant impact of ChatGPT on cyber security practices in Arab countries**.** To validate this hypothesis, linear regression analysis was used as follows

Table No (5) Impact of ChatGPT on cyber security practices

Independent variable	R	R^2	F		Sig
ChatGPT	.746[a]	.556	111.495	.000b	Statistically significant

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (42-52), Month: October - December 2023, Available at: www.researchpublish.com

As seen from the previous table, there was a statistically significant impact at the significance level of (0.05) for ChatGPT on cyber security practices in Arab countries as (R) value has reached (.746[a]) with a significance level of (.000b). This can be attributed to the viewpoint that Arab people may use ChatGPT for identifying new methods that can be used to enhance cybersecurity and protect personal and organizational information.

3.2.2 Verifying the second hypothesis: There is a statistically significant impact of ChatGPT on social engineering attacks in Arab countries. To validate this hypothesis, linear regression analysis was used as follows

Table No (6) Impact of ChatGPT on social engineering attacks

Independent variable	R	R^2	F		Sig
ChatGPT	.745a	.555	110.833	.000b	Statistically significant

As evident from the preceding table, there was a statistically significant impact of ChatGPT on social engineering attacks in Arab countries, with a significance level of (0.05). This significance is underscored by the strong positive correlation coefficient (R) value of (.745a) and an exceptionally low significance level of (.000b).

This finding can be attributed to the perspective that the utilization of ChatGPT may potentially contribute to an uptick in cyberattacks. It could facilitate the exploitation of social engineering techniques, such as persuasion, fabrication, and data gathering, which cybercriminals may leverage to compromise the security of digital systems and data in Arab countries.

4. DISCUSSION

The utilization of ChatGPT in Arab countries has elicited a moderate response, indicating that while Arab users are aware of this technology, they may not possess comprehensive knowledge regarding its diverse applications, particularly concerning its legal and illegal uses. This observation aligns with the assertion made by Shaer et al. (2023), who emphasize that the adoption of GPT technology in Arab countries is still in its nascent stages, given its status as an emerging technology. Dash & Sharma (2023) further underscore the importance of understanding both the potential advantages and disadvantages of ChatGPT.

In the domain of cybersecurity practices, a moderate response degree was also observed. This suggests that there may be room for improvement and greater emphasis on cybersecurity practices, particularly regarding the stringent implementation of security standards and regulatory frameworks. A robust legal framework is essential to act as a deterrent against those who seek to violate the security and privacy policies of cyberspace. This finding is in line with the insights provided by Shaer et al. (2023), who stress that cybersecurity issues constitute emerging research domains warranting further discussion and investigation in the Arab region.

The research results identified persuasion, fabrication, and data gathering as the primary techniques employed in social engineering attacks in Arab countries. This finding corroborates the assertion made by Alsulami et al. (2021), who highlight that social engineers employ a variety of techniques to deceive users into granting unauthorized access.

Moreover, the research outcomes indicate a statistically significant impact of ChatGPT on cybersecurity practices and social engineering attacks in Arab countries. This corroborates findings from previous research papers such as those by McKee & Noever (2023), Bahrini et al. (2023), and Ananthachari & Singh (2023), which also emphasize the significant role of ChatGPT in influencing these domains.

In summary, the research results provide valuable insights into the awareness of ChatGPT, cybersecurity practices, and social engineering attacks in Arab countries, highlighting both the existing vulnerabilities and the potential impact of this technology on security practices and threats.

5. CONCLUSIONS

The rapid advancement of machine learning and artificial intelligence technologies has ushered in a new era in digital security, with ChatGPT emerging as a transformative tool in the field of cybersecurity. One of the most notable ways in which ChatGPT is reshaping cybersecurity is through advanced threat detection capabilities. However, it's crucial to acknowledge the concerns raised by IT specialists, particularly regarding the potential misuse of ChatGPT by social engineers for cybercriminal activities.

The current research paper has endeavored to empirically investigate the potential impact of ChatGPT on both cybersecurity and social engineering. It underscores the imperative for Arab countries to prioritize software technology and harness the power of artificial intelligence to bolster their cybersecurity defenses. Additionally, the need to safeguard security systems from the potential threats posed by social engineers wielding ChatGPT is emphasized.

In light of the findings, the researcher recommends several key actions:

1. Raising Awareness: There is a pressing need to increase awareness among users to mitigate the risks associated with information and personal data breaches. Users should be informed and educated about best practices for online security.

2. Technological Utilization: Encouraging the utilization of modern technologies to fortify networks and enhance the security of electronic transactions is crucial. This entails leveraging emerging technologies to bolster cybersecurity measures.

3. Research Endeavors: Promoting and supporting further research into the applications of ChatGPT and its implications for cybersecurity is essential. Such research initiatives can aid in harnessing the potential of ChatGPT for enhancing cybersecurity while mitigating its misuse for malicious purposes.

In conclusion, the overarching aim of these studies is to maximize the benefits of emerging technologies like ChatGPT, particularly in the realm of cybersecurity. By fostering a deep understanding of the technology and its underlying algorithms, it is possible to utilize machine learning algorithms effectively to analyze data, detect security threats, and respond swiftly to mitigate potential risks.

ACKNOWLEDGEMENTS

I would like to thank the journal referees for their helpful comments and suggestions.

Declaration of competing interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Copyright

REFERENCES

[1] Addington, S. (2023). *ChatGPT: Cyber Security Threats and Countermeasures*. Research paper, San Bernardino Valley College, California, United States of America.

[2] Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet, 11*(73), 1-16.

[3] Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does Awareness of Social Engineering Make Employees More Secure? *International Journal of Computer Applications, 177*(38), 45-49.

[4] Alharthi, D., & Regan, A. (2021). A Literature Survey And Analysis On Social Engineering Defense Mechanisms And Infosec Policies. *International Journal of Network Security & Its Applications (IJNSA), 13*(2), 41-61.

[5] Almutairi, B. S., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security, 13*(2022), 363-379.

[6] Alsulami, M.H.; Alharbi, F.D.; Almutairi, H.M.; Almutairi, B.S.; Alotaibi, M.M.; Alanzi, M.E.; Alotaibi, K.G.; Alharthi, S.S. Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information, 12*(208), 1-13.

[7] Al-Wahaibi, D. S. S. (2022). *Investigating the factors influencing employees' intention toward avoiding social engineering threat in the Sultanate of Oman* (Unpublished Master Dissertation), Sultan Qaboos University, Sultanate of Oman.

[8] Ananthachari, P., & Singh, G. (2023). Repercussion of ChatGPT in Cybersecurity. *International Journal of Research Publication and Reviews, 4*(2), 1429- 1430.

[9] Bahrini, A., Khamoshifar, M., Abbasimehr, H., Riggs, R. J., Esmaeili, M., Majdabadkohne, R. M., &Pasehvar, M. (2023). *ChatGPT: Applications, Opportunities, and Threats*. IEEE Systems and Information Engineering Design Symposium (SIEDS) 2023.

[10] Borkovich, D. J., &Skovira, R. J. (2019). Cybersecurity Inertia And Social Engineering: Who's Worse, Employees Or Hackers? *Issues in Information Systems, 20*(13), 139-150.

[11] Breda, F., Barbosa, H., &Morais, T. (2017). *Social Engineering And Cyber Security*. In proceedings of "International Technology, Education and Development" Conference, 2017.

[12] Chakraborty, A., Biswas, A., & Khan, A. K. (2022). *Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation*. Springer Publications.

[13] Council of the European Union. (2023). ChatGPT in the Public Sector – overhyped or overlooked? European Union.

[14] Dash, B., & Sharma, P. (2023). Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review. *International Journal of Engineering and Applied Sciences (IJEAS), 10*(1), 1-5.

[15] Dave, T., Athaluri, S. A., & Singh, S. (2023). ChatGPT in medicine: an overview of its applications, advantages, limitations, future prospects, and ethical considerations. *Front. Artif. Intell., 6*(2023), 01-05.

[16] Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *I. J. Computer Network and Information Security, 1*(2017), 1-11

[17] Fitria, T. N. (2023). Artificial intelligence (AI) technology in OpenAIChatGPT application: A review of ChatGPT in writing English essay. *ELT FORUM 12*(1), 44-58.

[18] Fraiwan, M., &Khasawneh, N. (2023). A Review of ChatGPT Applications in Education, Marketing, Software Engineering, and Healthcare: Benefits, Drawbacks, and Research Directions. *Computers and Society*, 2022, 1-22.

[19] Grbic, D. V., & Dujlovic, I. (2023). *Social engineering with ChatGPT*. Proceedings of 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina.

[20] Gill, S. S., & Kaur, R. (2023). ChatGPT: Vision and challenges. *Internet of Things and Cyber-Phycial Systems, 3*(2023), 262-271.

[21] Haleem, A., Javaid, M., & Singh, R. P. (2022). An era of ChatGPT as a significant futuristic support tool: A study on features, abilities, and challenges. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2*(2022), 1-8.

[22] Hove, L. T. (2020). *Strategies Used to Mitigate Social Engineering Attacks* (Unpublished Doctor Dissertation), Walden University, Minneapolis, Minnesota.

[23] Inozemtsev, V., Ivleva, M., & Ivlev, V. (2017). Artificial Intelligence and the Problem of Computer Representation of Knowledge. *Advances in Social Science, Education and Humanities Research, 124*, 1151-1157.

[24] Kalla, D., & Smith, N. (2023). Study and Analysis of Chat GPT and its Impact on Different Fields of Study. *International Journal of Innovative Science and Research Technology, 8*(3), 827-833.

[25] Klimburg-Witjes, N., &Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology, & Human Values, 46*(6), 1316-1339.

[26] Maraj, A., & Butler, W. (2022). Taxonomy of Social Engineering Attacks: A Survey of Trends and Future Directions. Proceedings of the 17th International Conference on *Information Warfare and Security*, 2022, 185-193.

[27] McKee, F., &Noever, D. (2023). The Evolving Landscape Of Cybersecurity: Red Teams, Large Language Models, And The Emergence Of New Ai Attack Surfaces. *International Journal on Cryptography and Information Security (IJCIS), 13*(1), 1-34.

[28] Mijwil, M. M., Aljanabi, M., & Ali, A. H. (2023). ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. *Mesopotamian journal of Cybersecurity, 2023*, 18-21.

[29] Morovat, K., & Panda, B. (2020). *A Survey Of Artificial Intelligence In Cybersecurity*. International Conference on Computational Science and Computational Intelligence (CSCI), 2020, 109-115.

[30] O'Rourke, M. (2023). CHATGPT Poses Cybersecurity Threats. *Shutterstock/Tada Images*, 2023, p. 30.

[31] Oche, J. O. (2019). The Risk of Artificial Intelligence in Cyber Security and the Role of Humans. *Texila International Journal of Academic Research*, (Special Issue), 1-6.

[32] Pietikäinen, M., & Silvén, O. (2021). *Challenges of Artificial Intelligence: From Machine Learning And Computer Vision To Emotional Intelligence*. Finland: Center for Machine Vision and Signal Analysis.

[33] Rahman, M., &Watanobe, Y. (2023). ChatGPT for Education and Research: Opportunities, Threats, and Strategies. *Appl. Sci., 13*(2023), 1-21.

[34] Ray, P. P. (2023). ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. *Internet of Things and Cyber-Physical Systems, 3*(2023), 121-154.

[35] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. *International Journal of Engineering Research and Advanced Technology (IJERAT), 6*(5), 1-7.

[36] Sebastian, G. (2023). Do ChatGPT and Other AI Chatbots Pose a Cybersecurity Risk? An Exploratory Study. *International Journal of Security and Privacy in Pervasive Computing, 15*(1), 1-11.

[37] Shaer, S., O'Neil, A., Salem, F., Akrout, Z., &Shibl, E. (2023). *Advancing Artificial Intelligence Impact In Dubai Future Directions Toward Strengthening The Digital Economy*. Mohammed Bin Rahid School of Government, United Arab Emirates.

[38] Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences, 12*(2022), 1-19.

[39] Snyder, C. (2015). *Handling Human Hacking Creating a Comprehensive Defensive Strategy Against Modern Social Engineering* (Unpublished Academic Dissertation), Liberty University, Lynchburg, Virginia.

[40] The Global Cyber Security Capacity Centre. (2023). Global cyber security. Oxford Martin School, University of Oxford. https://www.oxfordmartin.ox.ac.uk/

[41] The World Bank Group. (2019). *Lessons Learned and Recommendations towards strengthening the Program: Global Cybersecurity Capacity Program*. The World Bank Group Publications.

[42] Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE, 8*(2020), 85094- 85115.

[43] Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, (2021), 1-21.

[44] Wilson, S. (2023). *Cybersecurity and Artificial Intelligence: Threats and Opportunities*. Contrast Security Publications Inc., Los Altos, California.