ChatGPT and Cybersecurity Education: Exploring the Challenges and Promises of

AI-Enabled Learning

A picture containing emblem, symbol, crest, badge

Description automatically generated***Abstract***

Amer Samamah

Tafila Technical University

smamhamr014@gmail.com

Hamzah Klaybat

Tafila Technical University

dreamhuntersa2000@yahoo.com

Dr. Khalid Alemerien

Tafila Technical University

khalidalemerien@gmail.com

Osama Jaradat

Tafila Technical University

osojr2017@gmail.com

Ahmad Mobarak

Tafila Technical University

ahmad101hamed@gmail.com

***With the development of artificial intelligence technology and the emergence of ChatGPT, which has caused a great revolution in all fields, especially the field of education and learning, we focused in our research on the power of ChatGPT in teaching and learning cybersecurity The main problem that our research focused on is that the chat is not connected to the Internet, and therefore it is not aware of developments and security gaps that are discovered daily in cybersecurity, therefore, in our experience, we used a questionnaire for local university students who study technology, especially cyber security, to answer a set of questions related to what we are looking at, and these questions depended on factors they were classified into 5-factors: Technology, Workflow and organization, Quality control, Maintenance and optimization, Training and skill level. Our results were as follows: We gained a highly satisfiable results based on the participants whose relying on ChatGPT to learn Cybersecurity ( as shown in Fig.4 ) the ability of ChatGPT to evolve is growing up day by day till it has the most necessary knowledge people rely on.***

**Keywords**: artificial intelligence;AI-enabled;learning; cybersecurity;ChatGPT;online learning; cybersecurity learning;

# Introduction

I

**n** recent years, cybersecurity has become an increasingly critical concern for individuals, businesses, and governments alike. According to Microsoft, nearly 80% of nation-state attackers targeted government agencies, thinks tanks and other non-government organizations [[1](https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/)] With the rise of digital technologies, cyber threats have become more sophisticated, widespread, and damaging. Despite the growing importance of cybersecurity, however, many people remain unaware of the risks they face and lack the knowledge and skills needed to protect themselves and their data. This has created a pressing need for effective cybersecurity education and learning programs. Analysis conducted using WebQDA software showed a positive understanding by the students of the use possibilities of the Chatbot as a resource on education, along with possible limitations of this learning resource [[12](https://library.iated.org/view/LOURENCO2023CHA)]. At the same time, recent advancements in artificial intelligence (AI) and natural language processing (NLP) have opened up new possibilities for education and learning. One such technology is ChatGPT [[15](https://openai.com/blog/chatgpt)] a large language model developed by OpenAI. Unlike previous chatbots, the latest ChatGPT model from OpenAI supports an advanced understanding of complex coding questions [[13](https://arxiv.org/abs/2212.11126)]. ChatGPT uses deep learning algorithms to generate human-like responses to text input making it a potentially powerful tool for personalized and interactive learning. While ChatGPT offers many benefits for cybersecurity education, there are also some limitations to consider. ChatGPT is still a machine learning model and may not be able to handle all cybersecurity-related scenarios or provide a comprehensive understanding of all threats. One surprising feature of ChatGPT as a language-only model centers on its ability to spawn coding approaches that yield images that obfuscate or embed executable programming steps or links [[13](https://arxiv.org/abs/2212.11126)]. by leveraging the vast amounts of data generated by ChatGPT's interactions, developers can create language models that are highly tuned to the specific needs and preferences of each There is always a risk of cybersecurity breaches or attacks on the ChatGPT system itself, which could compromise the security of user data. One of the challenges of cybersecurity education is the constantly evolving nature of cyber threats. Hackers are always developing new techniques and tactics, which means that cybersecurity education must be continuously updated to keep up with the latest trends. ChatGPT can help address this challenge by providing real-time updates on emerging cyber threats and offering personalized guidance on how to mitigate these risks.  
  
The aim of this research to explore the effectiveness of ChatGPT in Cyber Security education. is to investigate the potential applications, challenges, and benefits of using ChatGPT, an AI language model, in the context of cybersecurity education. The paper explores how AI-enabled learning, specifically through the use of ChatGPT, can contribute to cybersecurity education by enhancing learning experiences, providing interactive and personalized instruction, and addressing the specific challenges and requirements of cybersecurity training.

Osama Shawish

Tafila Technical University

shawishosama187@gmail.com

The work in the paper is organized as follows: Section II reviews Previous work in this field. Section III The methodology employed in this research paper aims to address the problem statement of effective cybersecurity education and learning programs through the utilization of ChatGPT, a large language model developed by OpenAI. The research will be guided by the following components: problem statement, research question, hypotheses, research model, and evaluation measures. Lastly, In the conclusion, the paper will provide recommendations for future research and highlight the transformative potential of ChatGPT and AI-enabled technologies in cybersecurity education and learning. It will offer insights into the evolving landscape of education in the age of AI trends are given in Section IV.

# Related Work

There are many studies and research papers related to cyber security education and learning. Some of these studies have explored the challenges associated with teaching cyber security, such as the lack of resources and the difficulty of keeping up with constantly evolving threats. Other studies have looked at different approaches to cyber security education, such as using hands-on training or gamification techniques. Some of the works focuses on threats and vulnerability analysis using several techniques. natural language processing (NLP) techniques have been increasingly applied to the field of cybersecurity to enhance various security tasks such as intrusion detection, threat intelligence, and security assessment. Meanwhile, the emergence of large language models like ChatGPT has enabled new opportunities for learning cybersecurity via natural language conversations. More specifically, in the context of using ChatGPT for learning cybersecurity, there have been several recent studies that have shown promising results. For example, the author in [4] proposed a cybersecurity education framework that utilizes ChatGPT as a conversational agent to provide personalized and interactive learning experiences for novice learners. The study demonstrated that the ChatGPT-based system was effective in improving learners' knowledge and skills in various cybersecurity topics. Similarly, [5] developed a ChatGPT-based system that can generate natural language explanations for cybersecurity concepts and scenarios. The system was trained on a large corpus of cybersecurity-related texts and can answer questions and provide explanations in a conversational manner. The authors evaluated the system on a dataset of cybersecurity questions and found that it achieved high accuracy and naturalness in generating responses. McKee et al. [13] utilized ChatGPT as an experimental platform to investigate cybersecurity issues. They modeled five different modes of computer virus properties, including self-replication, self-modification, execution, evasion, and application, using ChatGPT. These five modes encompassed thirteen encoding tasks from credential access to defense evasion within the MITRE ATT&CK framework. The results showed that the quality of ChatGPT's generated code was generally above average, except for the self-replication mode, where it performed poorly. They [24] also employed Chat-GPT as a network honeypot to defend against attackers. By having ChatGPT mimic Linux, Mac, and Windows terminal commands and providing interfaces for TeamViewer, nmap, and ping, a dynamic environment can be created to adapt to attackers' operations, and logs can be used to gain insight into their attack methods, tactics, and procedures. The authors demonstrated ten honeypot tasks to illustrate that ChatGPT's interface not only provides sufficient API memory to execute previous commands without defaulting to repetitive introductory tasks but also offers a responsive welcome program that maintains attackers' interest in multiple queries.  
The article [16] contributed to presenting the most important practices and procedures that must be taken into account in their performance to protect the digital environment from cyber-attacks. Modern methods must be utilized to improve the mechanisms operated by companies while educating employees about the seriousness and threats of cyberspace. And [17] how easily ChatGPT could be misused and concluded that this AI might pass the courses required for a university degree. [10] found that ChatGPT is able to provide correct or partially correct answers to 55.6% of questions. Moreover, ChatGPT is a poor judge of its own correctness: its confidence has little bearing on the correctness of its response. What was valuable on [6] has presented a CS threat and vulnerability assessment methodology based on ML Natural Language Processing approaches, specifically developed with the purpose of securing the HCII and, more in general, of the whole healthcare ecosystem and its supply chains. The survey of ChatGPT and GPT-4,state of the art large language models (LLM) from the GPT series, and their prospective applications across diverse domains [22]. Indeed, key innovations such as largescale pretraining that captures knowledge across the entire world wide web, instruction finetuning and Reinforcement Learning from Human Feedback (RLHF) have played significant roles in enhancing LLMs’ adaptability and performance.

Overall, these studies demonstrate the potential of ChatGPT in enhancing cybersecurity education and training through personalized and interactive learning experiences. However, further research is needed to explore the effectiveness of ChatGPT in different learning contexts and to address challenges such as data privacy and security in NLP-based systems.

[](https://drive.google.com/file/d/13VKMBgMx0vl_cLkNBKCKydYfJgD7uONW/view)Table 1: Related Work Summary

# Methodology

* Problem Statement

The introduction of AI-enabled learning technologies like ChatGPT offers a chance to overcome these constraints by offering tailored and interactive learning experiences. Despite the potential benefits of incorporating AI-enabled learning tools into cybersecurity education, it is uncertain if they are helpful in enhancing learners' knowledge, abilities, attitudes, perceptions, and behavior regarding cybersecurity and data privacy.

Proposed Solution:   
As a result, the purpose of this study is to investigate the influence of ChatGPT on learners' cybersecurity knowledge, skills, attitudes, perceptions, and behavior. The study will provide insights into the potential of AI-enabled learning tools in cybersecurity education and contribute to the development of effective and efficient cybersecurity education strategies. in order to better understand the problems and opportunities of AI-enabled learning in cybersecurity education.

* Research Question(s)

1. Can Chat GPT evolve to be fully relied upon in cybersecurity education?
2. Is there a significant difference in the effectiveness of cybersecurity education between learners who use AI-enabled learning tools (e.g., ChatGPT) and learners who do not use such tools?
3. Does the use of AI-enabled learning tools (e.g., ChatGPT) affect learners attitudes and perceptions towards cybersecurity and data privacy?

* Hypotheses

The following hypotheses are proposed for investigation:

H0: ChatGPT will evolve to the point where they are fully relied upon for cyber security education?

H1: ChatGPT will not evolve to the point where they are fully relied upon for cyber security education?

H0: There is a significant difference in the effectiveness of cybersecurity education between learners who use AI-enabled learning tools (e.g., ChatGPT) and learners who do not use such tools.

H1: There is no a significant difference in the effectiveness of cybersecurity education between learners who use AI-enabled learning tools (e.g., ChatGPT) and learners who do not use such tools.

H0: The use of AI-enabled learning tools (e.g., ChatGPT) does affect learners' attitudes and perceptions towards cybersecurity and data privacy.

H1: The use of AI-enabled learning tools (e.g., ChatGPT) does not affect learners' attitudes and perceptions towards cybersecurity and data privacy.

* Research Tool

The research employs quantitative and data collection method. The quantitative component involves the use of surveys of ChatGPT in cybersecurity education. survey questions to explore students' experiences, perceptions, and concerns related to using ChatGPT.

* Evaluation Measures

The following evaluation measures will be used to assess the effectiveness of ChatGPT for cybersecurity education:

By using [SPSS](https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower), a tool that computes statistical analyses for many different t tests, F tests, χ2 tests, z tests and some exact tests. SPSS can also be used to compute effect sizes and to display graphically the results of power analyses.

Measures of engagement with the ChatGPT system during the training, such as the number and duration of conversations and the quality of interactions.

By using the [google survey form](https://docs.google.com/forms/d/e/1FAIpQLSdwiWj1Ct5udPCBg6czeGcxS9L_cY8o9Xyoo-Tjzx7ISO6EPQ/closedform), the statistical results provide a comprehensive assessment of the effectiveness of ChatGPT for cybersecurity education and how significant is it.

# Experimental Results

This section elaborates the effectiveness of ChatGPT in cybersecurity learning using a google forms survey questionnaire.

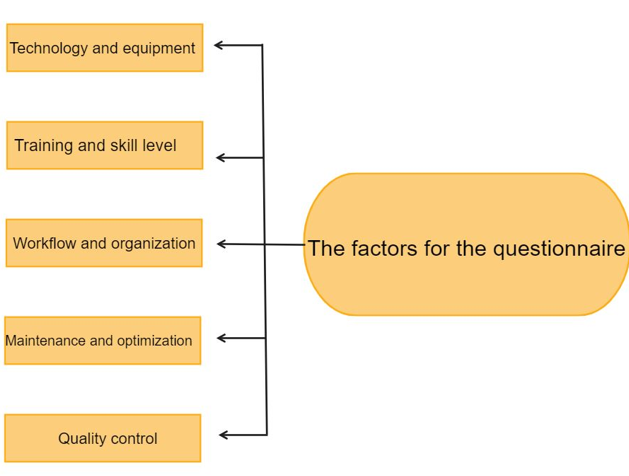


Fig. 1: Factors of Questionnaire

We used 17 questions related with cybersecurity learning on ChatGPT. We made a model defines the factors of the questionnaire shown in Fig.1 and gathered 83 responses with Cronbach alpha test of 0.831 reliability statistic using the below formula (F1), Where (a) is the coefficient alpha, (N) is the number of items, (C) is the covariance between item pairs and (v) is the average covariance.

F1: Chronbach alpha formula



The results were taken from many majors, as shown in Fig.2 The maximum number of the majors selected was cybersecurity.

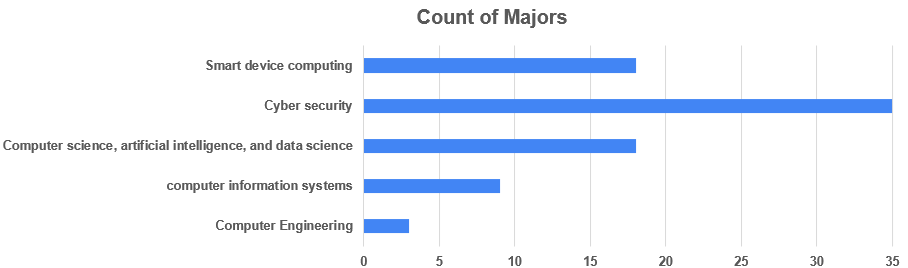
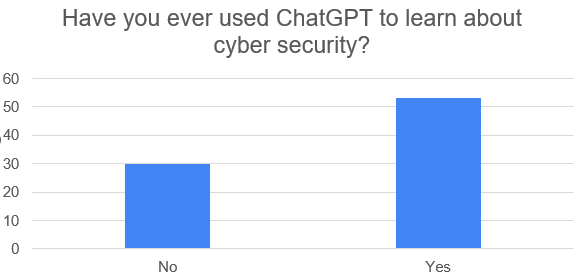


Fig. 2: Count of majors

This will increase the reliability of the conclusions due to the number of cybersecurity major participants.  
The most effective questions that provided answers to our hypothesis were taken based on the below figures.

Fig. 3: Using ChatGPT to learn about cybersecurity

In Fig.3, participants confirmed that the presented technology ChatGPT is efficient in their learning process. This confirms our (RQ1).

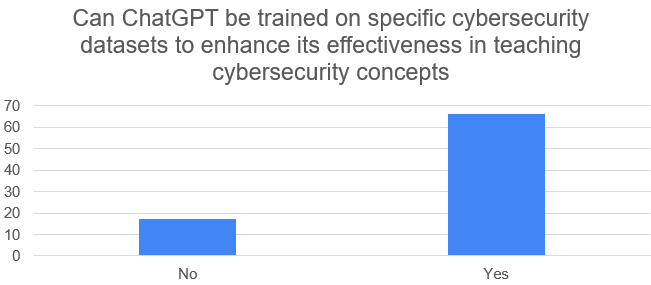


Fig. 4: ChatGPT trained datasets effectiveness

The above Fig.4 results a good analysis on the evolve of ChatGPT’s ability to provide a better interaction with the users. This admits the first hypothesis of the research paper where ChatGPT will evolve to be fully reliable in cybersecurity learning.

One of the good questions was talking about ChatGPT’s ability to provide the user with the necessary knowledge and skills to enhance his understanding of cybersecurity concepts. The results were negative that’s due to [18] ChatGPT allows for easy cheating in the school and university environment. Correct answers to exam questions or functional pieces of code are available with a few clicks. This easy access to correct solutions can vastly reduce the learning experience that students should undergo. Using the ChatGPT will stop original content creation. The same goes for programming. Using the ChatGPT to generate code vastly reduces the knowledge and experience students gain while solving the assigned problem.

This confirms the second hypothesis and the (RQ2) but in a negative direction where students will have lack of knowledge because of the high usage of ChatGPT.

As for data privacy attitudes, most participants weren’t very satisfied in ChatGPT’s data privacy; 51.8% positive vs. 48.2% negative answers given in terms of privacy, this denies the third hypothesis and admits our (RQ3) we declared as it proofs that people still have concerns about privacy and security on the wide world network.

In conclusion, ChatGPT has shown great promise in the field of education, particularly in programming learning. However, more research is needed to fully understand the potential benefits and challenges of using ChatGPT in education.

# Conclusion And Future Work

In conclusion, ChatGPT can enhance the learning experience and interaction with students. However, we must be cautious not to rely excessively on ChatGPT, as it may lead to cheating and hinder original thinking and problem-solving skills. Data privacy concerns were also evident among participants.

In the future, this work might be extended for The effectiveness of ChatGPT in teaching cybersecurity, especially Network engineering.

# Acknowledgement

We would like to express our very great appreciation to Dr. Khalid Alemerien for his valuable and constructive suggestions during the planning and development of this research paper. His willingness to give his time so generously has been greatly appreciated.

# References

1. Lambert, J. (2021, October). Microsoft Digital Defense Report shares new insights on nation-state attacks.
2. Farrokhnia, M., Banihashem, S. K., Noroozi, O., & Wals, A. (2023, March). A SWOT analysis of ChatGPT implications for educational practice and research. Journal of Innovations in Education and Teaching International.
3. Megahed, F. M., Chen, Y.-J., Ferris, J. A., Knoth, S., & Jones-Farmer, L. A. (2023, February). How Generative AI models such as ChatGPT can be (Mis)Used in SPC Practice, Education, and Research? An Exploratory Study. arXiv 2023, arXiv:2302.10916.
4. Dogan, M. E., Dogan, T. G., & Bozkurt, A. (2022, October). A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. In Proceedings of IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece.
5. Mijwil, M. M., Aljanabi, M., Ali, A. H., & Mijwil, 19. (2023, January). Exploring the Role of Cybersecurity in the Protection of Medical. Mesopotamian Journal of Cybersecurity, Vol 18–21.
6. Mijwil, M. M., Aljanabi, M., & ChatGPT3. (2023, January). Towards Artificial Intelligence-Based Cybersecurity: Practices and ChatGPT Generated Ways to Combat Cybercrime. Iraqi Journal for Computer Science and Mathematics.
7. Biswas, S. S. (2023, March). Role of ChatGPT in Cybersecurity, Artificial Intelligence eJournal, Tennessee, USA.
8. Jalil, S., Rafi, S., LaToza, T. D., Moran, K., & Lam, W. (2023). ChatGPT and Software Testing Education: Promises & Perils, 2023 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 8 pages, 2 tables, 6 figures, Fairfax, USA.
9. Sharma, P., & Dash, B. (2023, March). Impact of Big Data Analytics and ChatGPT on Cybersecurity: Conference Paper, Conference: IEEE 4th INTERNATIONAL CONFERENCE ON COMPUTING AND COMMUNICATION SYSTEMS (I3CS), NEHU, Shillong.
10. Lourenço, J., Morais, M. Lousã, Sá. (2023). Chatbot As A New Lecturing Tutor: Challenges In Lecturing And In Cybersecurity. In 17th International Technology, Education and Development Conference. Springer, Cham.
11. McKee, F., & Noever, D. (2022, December). Chatbots in a Botnet World. International Journal of Engineering and Applied Sciences (IJEAS), 10(1).
12. Aljanabi, M. (2023, January). ChatGPT: Future Directions and Open possibilities, Mesopotamian Journal of Cyber Security, Baghdad, Iraq.
13. OpenAI. (2023). ChatGPT.
14. Mijwil, M. M., Filali, Y., Aljanabi, M., Bounabi, M., Al-Shahwani, H., & ChatGpt. (2023, January). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment, Mesopotamian journal of Cybersecurity.
15. Malinka, K., Perešíni, M., Firc, A., Hujňák, O., Januš, F. (2023, March). On the Educational Impact of ChatGPT: Is Artificial Intelligence Ready to Obtain a University Degree?, arXiv:2303.11146.
16. GitHub. (2022). GitHub Copilot.
17. Rees, K. (2023, January). ChatGPT used by Cybercriminals to write malware.
18. NL Times. (2023). Dutch Students using ChatGPT to finish homework; Teachers aren't noticing.
19. Rosenblatt, K. (2023). ChatGPT banned from New York City public schools' devices and networks.
20. Liu, Y., Han, T., Ma, S., Zhang, J., Yang, Y., Tian, J., … Ge, B. (2023). Summary of ChatGPT/GPT-4 Research and Perspective Towards the Future of Large Language Models. arXiv preprint arXiv:2304.01852.
21. Syme, P. (2023). A Princeton student built an app which can detect if ChatGPT wrote an essay to combat AI-based plagiarism. Business Insider.
22. McKee, F., & Noever, D. (2023, February). Chatbots in a Honeypot World. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-12).
23. Dash, B., & Sharma, P. (2023, January). Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review. International Journal of Engineering and Applied Sciences (IJEAS), 10(1).
24. Addington, S. (2023, April). ChatGPT: Cyber Security Threats and Countermeasures. San Bernardino.
25. MDPI. (2022). ChatGPT for Education and Programming Learning: Opportunities and Challenges. Applied Sciences, 13(9), 5783.
26. Cambridge University. (2023, April 5). ChatGPT: opportunities and challenges for education.