ChatGPT and Cybersecurity Education: Exploring the Challenges and Promises of

AI-Enabled Learning

A picture containing emblem, symbol, crest, badge

Description automatically generated\_***Abstract***

Hamzah Klaybat

Tafila Technical University

dreamhuntersa2000@yahoo.com

Dr. Khalid Alemerien

Tafila Technical University

khalidalemerien@gmail.com

Amer Samamah

Tafila Technical University

smamhamr014@gmail.com

Osama Jaradat

Tafila Technical University

osojr2017@gmail.com

Ahmad Mobarak

Tafila Technical University

ahmad101hamed@gmail.com

Keywords: artificial intelligence; cybersecurity; large-language models; ChatGPT; online learning; Computer Security

# 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 user, leading to a more personalized and engaging experience [[14](https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/33)]. Additionally, while this technology might be misused for

cheating, there are also implications for technical fields, especially computer science, as it can simplify creative activities such as programming. A good example might be the GitHub Copilot [[18](https://github.com/features/copilot)] known as the first cases of malware created using ChatGPT [[19](https://www.makeuseof.com/chatgpt-used-by-cybercriminals-to-write-malware/)]. The student’s ability to adopt this technology to subvert the text produced by ChapGPT proved to be particularly good and fast. Dutch students have already admitted to using this technology to write homework [[20](https://nltimes.nl/2023/01/16/dutch-students-using-chatgpt-finish-homework-teachers-arent-noticing)]. And as confirmed cases of cheating began to emerge very quickly, the reaction in the education system was similarly swift. For example, New York City schools immediately banned this technology in the classrooms [[21](https://www.nbcnews.com/tech/tech-news/new-yorkcity-public-schools-ban-chatgpt-devices-networks-rcna64446)]. On the other hand, the first tools to detect ChatGPT-generated texts started to appear [[23](https://www.businessinsider.com/app-detects-if-chatgpt-wrote-essay-ai-plagiarism-2023-1)]. 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.

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. In the area of NLP-based cybersecurity, numerous studies have been conducted to investigate the application of machine learning and deep learning algorithms for detecting anomalies, identifying malicious patterns, and predicting attacks in network traffic data [2]. Furthermore, researchers have also explored the use of NLP techniques for analyzing text data from social media, dark web forums, and other sources to identify cyber threats and vulnerabilities [3]. 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 paper [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 interfacesfor 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. [22] 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. 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.

# 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.

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)

Can Natural Language Processing and Chat GPT evolve to be fully relied upon in cybersecurity education?

* Hypotheses

The hypotheses for this study are:

H0: Natural Language Processing and GPT chat will not evolve to the point where they are fully relied upon for cyber security education?

* Research Model

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 [G\*Power](https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower), a tool that computes statistical power analyses for many different t tests, F tests, χ2 tests, z tests and some exact tests. G\*Power 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://forms.gle/HeenULZpREbyLaZeA), the statistical results provide a comprehensive assessment of the effectiveness of ChatGPT for cybersecurity education and how significant is it.

# References

1. John Lambert. (2021, Oct). Microsoft Digital Defense Report shares new insights on nation-state attacks. Microsoft. Available: https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/

Last accessed in 20/April/2023.

1. [Dukka Reddy](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Reddy/Dukka+KarunKumar), [Himansu Behera](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Behera/Himansu+Sekhar), [Janmenjoy Nayak](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Nayak/Janmenjoy), [Pandi Vijayakumar](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Vijayakumar/Pandi), [Bighnaraj Naik](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Naik/Bighnaraj), [Pradeep Singh](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Singh/Pradeep+Kumar). (2020, Oct). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Wiley Online Library. Available:

<https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4121>. Last accessed in 20/April/2023.

1. Murat Ertan Dogan, Tulay Goru Dogan, and Aras Bozkurt. (2022, Oct). A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Available: <https://www.mdpi.com/1424-8220/23/2/651> Last accessed in 20/April/2023.
2. Mohammadreza Farrokhnia, Seyyed Kazem Banihashem, Omid Noroozi & Arjen Wals. (2023, Mar).A SWOT analysis of ChatGPT Implications for educational practice and research Available: <https://www.tandfonline.com/doi/full/10.1080/14703297.2023.2195846> Last accessed in : 20/April/2023.
3. Fadel M. Megahed, Ying-Ju Chen, Joshua A. Ferris, Sven Knoth and L. Allison Jones-Farmer. (2023, Feb). How Generative AI models such as ChatGPT (Mis)Used In SPC Practice, Education, And Research? An Exploratory Study. Available: [https://arxiv.org/abs/2302.10916 Last accessed in 20/April/2023](https://arxiv.org/abs/2302.10916%20Last%20accessed%20in%2020/April/2023).
4. Murat Ertan Dogan, Tulay Goru Dogan, and Aras Bozkurt. (2022, Oct). A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and

Vulnerabilities of the Healthcare Ecosystem. Available: <https://www.mdpi.com/1424-8220/23/2/651> Last accessed in 11/May/2023.

[7] Maad M. Mijwil,Mohammad Aljanabi,Ahmed Hussein Ali,19 Mijwil. (2023, Jan). Exploring the Role of Cybersecurity in the Protection of Medical: Mesopotamian Journal of Cybersecurity Vol.2023, 18–21. Available:

<https://journals.mesopotamian.press/index.php/CyberSecurity/article/view/29>. Last accessed in 11/May/2023.

[8] Maad M. Mijwil,Mohammad Aljanabi,ChatGPT3. (2023, Jan). Towards Artificial Intelligence-Based Cybersecurity: Practices and ChatGPT Generated Ways to Combat Cybercrime. Available: <https://doi.org/10.52866/ijcsm.2023.01.01.0019>. Last accessed in 11/May/2023.

[9] Dr. Biswas Som Subhro Biswas. (2023, Mar). Role of ChatGPT in Cybersecurity. Available: <https://ssrn.com/abstract=4403584>. Last accessed in 20/April/2023.

[10] Sajed Jalil,Suzzana Rafi,Thomas D. LaToza,Kevin Moran, Wing Lam. (2023, Mar). ChatGPT and Software Testing Education: Promises & Perils. Available: <https://arxiv.org/abs/2302.03287>

[11] Pawankumar Sharma, Bibhu Dash. (2023, Mar). Impact of Big Data Analytics and ChatGPT on Cybersecurity: Conference Paper.

Available: <https://www.researchgate.net/publication/369358499>. Last accessed in 11/May/2023.

[12] J. Lourenço, orcid J., Morais orcid. M. Lousã, orcid S., Sá orcid. “Chatbot As A New Lecturing Tutor: Challenges In Lecturing And In Cybersecurity” 17th International Technology, Education and Development Conference. Springer, Cham, 2023 Available: <https://library.iated.org/view/LOURENCO2023CHA>. Last accessed in 11/May/2023.

[13] Forrest McKee, David Noever. (2022, Dec). Chatbots in a Botnet World. Available: <https://arxiv.org/abs/2212.11126>.

[14] Mohammad Aljanabi (2023, Jan). ChatGPT: Future Directions and Open possibilities.

Available: [https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/33.](https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/33.%20)  Last accessed in 11/May/2023.

[15] OpenAI, “ChatGPT.” https://openai.com/blog/chatgpt, (2023). Last accessed in 11/May/2023.

[16] Mijwil M. M., Filali Y., Aljanabi M., Bounabi M., Al-Shahwani H., and ChatGpt (2023, Jan). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment Available: <https://www.researchgate.net/publication/367191397>.

Last accessed in 11/May/2023.

[17] Kamil Malinka, Martin Perešíni, Anton Firc, Ondřej Hujňák, Filip Januš (2023, Mar). On the Educational Impact of ChatGPT: Is Artificial Intelligence Ready to Obtain a University Degree? Available: <https://arxiv.org/abs/2303.11146>. Last Accessed In : 11/May/2023.

[18] GitHub. 2022. GitHub Copilot · Your AI pair programmer. https://github.com/features/copilot. Last Accessed In : 11/May/2023.

[19] Katie Rees. (2023, Jan). Chatgpt used by Cybercriminals to write malware. <https://www.makeuseof.com/chatgpt-used-by-cybercriminals-to-write-malware/>

[20] NL Times. 2023. Dutch Students using ChatGPT to finish homework; Teachersaren’t noticing. Available:

<https://nltimes.nl/2023/01/16/dutch-students-using-chatgptfinish-homework-teachers-arent-noticing>. Last Accessed In : 11/May/2023.

[21] Kalhan Rosenblatt. 2023. ChatGPT banned from New York City public schools’ devices and networks. Available:

<https://www.nbcnews.com/tech/tech-news/new-yorkcity-public-schools-ban-chatgpt-devices-networks-rcna64446>. Last Accessed In: 11/May/2023.

[22] Yiheng Liu, Tianle Han, Siyuan Ma, Jiayue Zhang, Yuanyuan Yang, Jiaming Tian, Hao He, Antong Li, Mengshen He, Zhengliang Liu, Zihao Wu, Dajiang Zhu, Xiang Li, Ning Qiang, Dingang Shen, Tianming Liu, Bao Ge. Summary of ChatGPT/GPT-4 Research and Perspective Towards the Future of Large Language Models Available: <https://arxiv.org/abs/2304.01852>.

Last Accessed In: 11/May/2023.

[23] Pete Syme. (2023). A Princeton student built an app which can detect if ChatGPT wrote an essay to combat AI-based plagiarism.   
Available: <https://www.businessinsider.com/app-detects-if-chatgpt-wrote-essay-ai-plagiarism-2023-1>. Last Accessed In: 11/May/2023.

[24] Forrest McKee, David Noever. (2023, Feb). Chatbots in a Botnet World. Available: <https://arxiv.org/abs/2301.03771>. Last Accessed In: 12/May/2023.