Generative AI – Promoting or Impeding Cybersecurity Education: A Capture the Flag Case Study

Heloise Meyer – South African National Research Network (SANReN), NICIS, CSIR

Generative Artificial Intelligence (AI) has taken the world by storm since the public release of ChatGPT, an AI-based chatbot, in November 2022. The first reactions were awe and amazement as ChatGPT presented the capability to respond to various text-based questions following a conversational approach. However, ChatGPT's ability to complete more advanced tasks, such as supplying source code to programming-related questions or generating complete articles focusing on a specific topic, has caused eyebrows to be raised. The capabilities offered by ChatGPT, fuelled by popularity and easy accessibility, have introduced several new challenges for the education sector. One such challenge is the concept of AI-assisted cheating, where students utilise chatbots, such as ChatGPT, to answer specific questions or complete assignments. Such cheating has become a concern during Capture the Flag (CTF) events. CTF events offer a popular platform to promote cybersecurity education, allowing students to gain hands-on experience solving cybersecurity challenges in a fun but controlled environment. Students partake in CTF events by either solving a collection of challenges (jeopardy-style) or defending their vulnerable system while attacking other teams' systems (attack-defence). The popularity of CTF events and their game-like setting has encouraged universities to incorporate CTF events as a form of cybersecurity education. One such initiative is the Cyber Security Challenge (CSC), first introduced in 2017 and organised by the South African National Research Network (SANReN).

The purpose of the CSC is to stimulate interest in cybersecurity and offer students an opportunity to receive exposure to current and trending cybersecurity topics. The expectation is that such exposure will stimulate interest in the field of cyber and information security, growing the next generation of cybersecurity specialists. Research studies have found that students exposed to the CSC have shown a significant increase in knowledge and interest in cybersecurity-related fields as a profession. The importance of CTF events, such as the CSC, is unquestionable and highlights the importance of students gaining practical experience in cybersecurity. However, the emergence of ChatGPT has raised concerns regarding the possible influence of technology on the learning ability offered by CTF events. ChatGPT is freely available and accessible to any student with a smartphone and Internet connectivity. Since the typical style of CTF challenges usually follows a question-answer format, it offers students the ideal opportunity to enlist the assistance of ChatGPT. The focus of this lightning talk will discuss the ability of ChatGPT to assist and aid students in solving CTF challenges. The purpose is to examine the assistance ChatGPT can offer to students participating in CTF competitions and whether structural changes to CTF challenges will be required.

The lightning talk will be of interest to all attendees from the research and education sector, eliciting discussions regarding the impact of generative AI technologies, such as ChatGPT, on Securing Tomorrow's Knowledge, namely growing the next generation of cybersecurity specialists. Are technologies, such as ChatGPT, impeding or promoting the teaching of cybersecurity? The learning ability offered by ChatGPT is invaluable since the chatbot can quickly interpret a question and present relevant information in a concise format. Students can, therefore, quickly grasp a concept or acquire a workable solution to a problem. However, the presented information is not always accurate or correct. Furthermore, the capabilities offered by ChatGPT can easily lead to "spoon-feeding", impacting critical thinking, should students fail to comprehend and fully understand the information presented by ChatGPT. These questions also relate to cybersecurity practitioners operating as incident responders, security strategists, or security management professionals. Is generative AI impeding critical thinking or is it an additional tool in the arsenal of security practitioners?