# A new approach to cybersecurity awareness: automated by OpenAI

# ABSTRACT

The current study aims to improve ongoing cybersecurity awareness programs by introducing a novel approach. This paper analyzes previous and ongoing cybersecurity awareness initiatives, delves into the advantages of security awareness programs, and outlines the most effective strategy for their implementation. The newly developed program is designed to encompass a variety of cybersecurity topics including password security, phishing awareness, social engineering, data privacy and social media use, as well as safe internet practices. In this program, OpenAI is utilized in this program to create an interactive module whereby users engage with multiple choice questions, receive feedback based on their response and proceed to a new question based on their answer. Being auto generated, each participant experiences a unique program. The program's effectiveness will be measured by comparing the results of participants who undergo this training with those exposed to cybersecurity video lessons.

**Introduction**

Security awareness continues to be of paramount importance worldwide as technology continues to evolve daily. Inevitably, as technology evolves, cyber threats consequently continue to progress rapidly. The rise of modern cyber threats demands an increase in security awareness among all users of technology. According to the National Institute of Standards and Technology (NIST), cybersecurity is defined as “the ability to protect or defend the use of cyberspace from cyber-attacks.” **(CITE)** Similarly, cybersecurity awareness as defined by (**CITE**), involves “the extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly.” This definition suggests that security awareness is intricately linked to behavior. Consequently, an individual who possesses awareness of information security is expected to exhibit behavior that reflects this understanding. Thus, cybersecurity awareness can be enhanced through education that enlightens individuals about information security and encourages the adoption of secure habits to protect against cyberattacks. Security habits can be defined as “learned sequences of acts that become automatic responses to specific situations which may be functional in obtaining certain goals or end states” (**Verplanken, Aarts and Van Knippenberg 1997; Limayem, Hirt and Cheung 2003**). The performance of these habits demand minimal mental effort and attention and are therefore performed almost automatically. By extension, security behavior can be defined by a continuous practice of these security habits. (**CITE**) Current initiatives to increase security awareness include training platforms such as Knowbe4 and Goldphish, poster campaigns offering security insights, accessible online guides, video game-based training, and informative online videos. This newly developed program adopts a new approach to security awareness by educating users through interactive security questions generated by OpenAI. Engaging in this training provides individuals with a unique, specialized learning experience designed to enhance their understanding of security awareness. Its goal is to strengthen their ability to spot cyber threats and instill secure practices to prevent potential cyberattacks they may face.

**Background and related work**

**Proposal**

**Partial implementation**

Initial research aimed to identify the top five cybersecurity attacks that college students fall for as well as five essential topics crucial for educating them to defend against these specific attacks. Analyzing past research and insights from Chat-GPT on this matter resulted in a finalized list of essential security topics: phishing awareness, password security, social engineering, data privacy and social media use, as well as safe internet use. These topics formed the basis for developing pre-test and post-test questions, which were created with the assistance of ChatGPT. These were designed to assess each participant's learning progress by comparing their knowledge before and after the training sessions.

Chat-gpt snippet:

Prompt: Generate 4 multiple-choice questions that would give insight into how much knowledge a person has about password security as well as an

idea of their current password creation processes/behaviors.

Answer:

Which of the following is considered a strong password?

a) Password123

b) P@ssw0rd!

c) MyDogL0vesP@ssw0rd$!

d) 12345678

The OpenAI playground was utilized to test Chat-4, assessing its suitability for this program and gaining an understanding of its expected operations behind the scenes throughout the training. However, initial experiments revealed inaccuracies: OpenAI couldn't reliably indicate correct or incorrect answers and didn't adhere to the system prompt's topic-switching requirements.

OpenAI playground snippet:

System: You are a cybersecurity specialist educating college students on cybersecurity awareness. You will ask them multiple choice (A, B, C, D) questions on 5 different topics (Phishing Awareness, Password Security, Social Engineering, Safe Internet Use and Data Privacy and Social Media Awareness). You will wait for the user to answer the question (they will answer with A B C or D) then create new questions based on their response. You will start a new topic only if they have answered 3 questions correctly for that topic. You will provide feedback after each response.

Assistant:

11. Which of the following is not a safe internet practice?

A. Ignoring software updates

B. Using strong and unique passwords

C. Regularly backing up critical data

D. Limiting the amount of personal information shared online

\*\*\*\*\*\*\*\*\*\*\*LET’S ANSWER QUESTION 3 WRONG TO SEE IF IT STAYS ON THE SAME TOPIC\*\*\*\*\*\*\*\*\*\*\*

User:

B

Assistant:

Good job! The correct answer is (A). Ignoring software updates is not a safe internet practice. Updates often contain important security patches that help protect your device and your information from new threats.

\*\*\*\*\*\*\*\*\*\*\*SAID THAT THE ANSWER WAS RIGHT WHEN IT WAS WRONG, CHANGED TO A NEW TOPIC FOLLOWING THIS\*\*\*\*\*\*\*\*\*\*\*

These initial experiments highlighted that OpenAI cannot be treated as an agent, and that it cannot maintain state. Subsequent trials involved treating OpenAI as a function by breaking down system prompts to consult OpenAI for single steps, assigning it one straightforward task at a time while manually managing state. Troubleshooting was conducted while experimenting with various temperatures which regulate OpenAI’s creativity, with a temperature of 0.5 proving to be of optimal efficiency. Upon achieving satisfaction, efforts transitioned to coding a python program to mirror the OpenAI playground experiments. A comprehensive code was developed to generate questions, receive user responses, provide feedback, and to initiate a new topic after either three correctly answered questions or completion of five questions within that topic. The code maintains records of correct answers and total questions answered to ensure optimal functionality.

**Conclusion**