It has been decided upon to have the interactive lessons of the project be generated by chat-gpt in the background of the application. The past few weeks have been spent troubleshooting chat-4 to gauge how useful it will be for this project. This experimentation is being carried out on the OpenAI playground platform using chat-4 (recommended by Dr. Eckroth and agreed upon by Dr. Plante and I). Initial experiments confused chat-4 as it would say answers were right when it was wrong, and it did not record how many questions were answered correctly before moving on to a new topic. This yielded results such as this:

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

\*\*\*\*\*\*\*\*\*\*\*SAME PROBLEMS OCCUR\*\*\*\*\*\*\*\*\*\*\*

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.

These initial prompts led to an understanding of how chat-4 cannot be treated as an agent and cannot maintain state. Since then, the goal has been to continue experimenting with chat-4, changing the system prompts to what is needed to yield the desired results. The code will be used to maintain a record of how many questions are answered correctly before introducing a new topic. New methods have improved chat’s responses, but some challenges are still noted.

Initial system prompt:

System:

You are a cybersecurity specialist educating college students on cybersecurity awareness. Let's begin by asking the user a multiple choice question (answer choices: A, B, C, D) on the topic of Phishing Awareness

\*\*\*\*\*\*\*\*\*\*\*WHERE CHAT MESSED UP\*\*\*\*\*\*\*\*\*\*\*

Assistant:

Let's move on to the next question:

What is an example of a social engineering attack?

A) Installing antivirus software on a computer

B) Sending spam emails to a large number of recipients

C) Pretending to be a bank representative and requesting account information

D) Conducting regular security awareness training for employees

Please choose the letter (A, B, C, or D) that represents the correct answer.

LETS CHECK IF ITLL RECOGNIZE A WRONG ANSWER AGAIN

System:

What is an example of a social engineering attack?

A) Installing antivirus software on a computer

B) Sending spam emails to a large number of recipients

C) Pretending to be a bank representative and requesting account information

D) Conducting regular security awareness training for employees

The user answered this question with option A. Give them feedback on their answer choice and generate a new multiple (A, B, C, D) choice question on this topic based on this.

NOPE, AND IT CREATED ANOTHER REGULAR QUESTION INSTEAD OF MULTIPLE CHOICE

Assistant:

You are correct! The correct answer is C) Pretending to be a bank representative and requesting account information. This is an example of a social engineering attack where an attacker tries to gain access to sensitive information by impersonating a trusted entity or organization.

Great job! Let's move on to the next topic: Malware.

What is malware and how does it affect computer systems?

This snippet reveals how chat still misreads the user’s response and struggles to continuously generate a multiple-choice question (as opposed to an open-ended question). Further experimentation will be done on the playground until chat-4 works as desired. Initial steps will involve breaking down prompts even more and giving chat simple and single tasks at a time. The ultimate goal is to have chat generate a multiple choice question, evaluate the user’s response, then give feedback based on the user’s response. The code will keep a record of how many questions have been answered correctly and will prompt chat-4 to generate questions on a new topic after three questions have been answered correctly for each topic.