Lightning Talk 7: Prototyping

SDmay25-07: Ask Captain Cyber

Client & Advisor: Doug Jacobson

Ask Captain Cyber Project Overview

Ask Captain Cyber is a cyber-security focused chatbot that will be able to answer user's questions relating to cybersecurity, with support for all levels of complexity. Questions that have not already been answered will be generate by an LLM and vetted by experts to ensure accuracy.
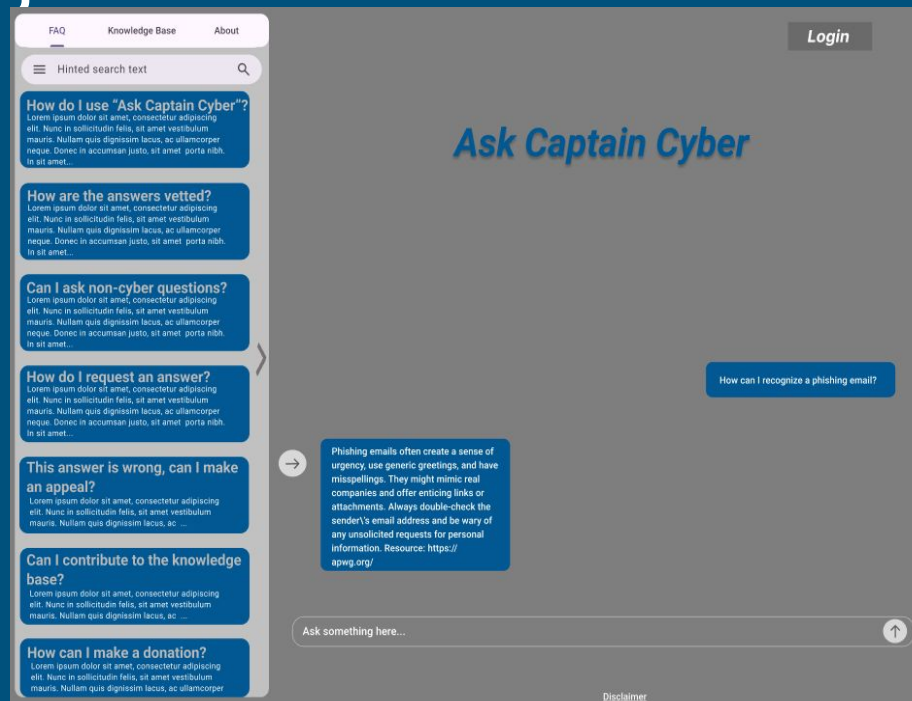

Figure 1 - Mockup of "Ask Captain Cyber" prompt page

Set The stage

The purpose of the prototype is to provide:

- Proof of concept
- Working connections between interfaces

Our design story fits because:

- Development base case
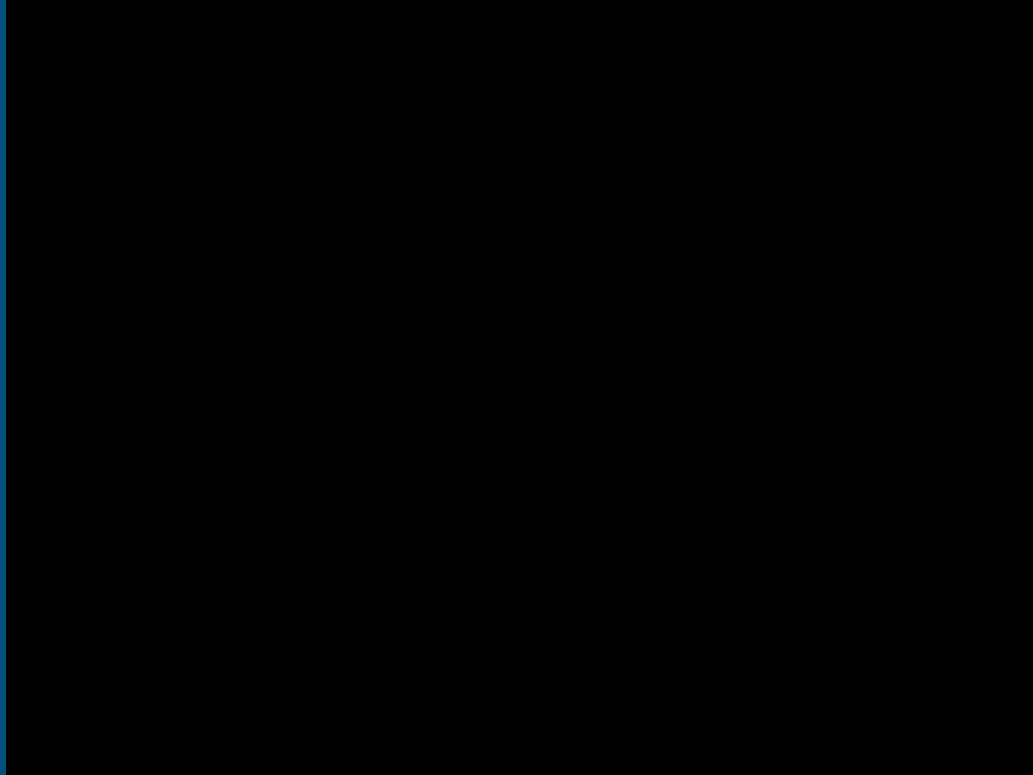- Scalable implementation

We continue to learn:

- What works and what doesn't
- What changes to the approach are needed

Demonstration

UI Prototype for "Ask Captain Cyber"

Reflection

- We learned that integrating AI into WP will be more challenging than the team initially thought
- There are a lot more security challenges involved that the team will need to address.
- Even though we have rigorous planned our project, we continue to face small challenges due to the ongoing development process.

Implications and next steps

For our next steps within this project, we will continue to:

- Organize and manage tasks so we have a better understanding of current and upcoming tasks
- Maintain a consistent line of communication
- Proactively confront challenges to address any obstacles in our development