A Cybersecurity Resource Hub for Mobile Users in Developing Countries

Teng Hui Yi Sarry

2721338T

Project Outline

Motivation

In developing countries, mobile devices are the primary way people access the internet. However, many users lack even basic knowledge of online safety and cybersecurity concepts, leaving them highly vulnerable to threats like phishing, malware, and identity theft. By offering simple guides and language-switching features, the platform will empower users to adopt safer online practices. This project contributes to enhancing digital literacy and fostering a secure online environment, particularly for vulnerable populations.

Aims

The project will develop a mobile-friendly website providing accessible resources for cybersecurity education in developing countries. This will include:

- Comprehensive guides on online safety and cybersecurity concepts, best practices and lists of free cybersecurity tools.

- Offers a seamless language-switching feature to make content accessible in at least two languages.

- Ensures compatibility across devices, including desktops, tablets, and smartphones.

- [If time permits] Interactive features such as quizzes to enhance learning

Progress

- Background research conducted

- Framework chosen:

    - Backend: Flask, (potentially API integration for translations – still undecided)

- Frontend: HTML, CSS, and JavaScript

- System architecture outlined

  - If database is required: A NoSQL database (e.g., Firebase) to store content, quizzes, and user data for future dynamic features.

- Core functionalities have been prioritized using the MoSCoW framework.

- Implementation progress:

  - Basic website structure created, with initial content displayed.

  - Rough styling done; needs refinement and responsiveness testing.

  - Multilingual support: Research ongoing into translation options, including APIs for automatic translation and manual translation with Babel.

Problems and risks

Problems

- deciding on the technologies to use as not proficient in coding and had concerns on what would be good for this project

- 2nd language dilemma – looking into the various methods available; either a manual translation of all the content or using an API to automatically translate

- All the pages are currently not responsive to size of device; looks better only on mobile devices

- All the content are currently not yet credited as well

Risks

- Not sure how to implement responsiveness for all devices. **Mitigation**: search online how to do responsive pages and try to adapt from there

- Not confident about automated testing methods, including CI/CD pipelines and unit tests. **Mitigation**: do research on how to get started on those, or perhaps ask peers who are strong in programming for advice

Plan

- Week 1-2: Refine website styling and implement content in at least two languages.

  - **Deliverable:** Fully styled and responsive website with content implemented in at least two languages, including a functional language-switching feature.

- Week 3-4: Integrate test quizzes and other interactive features

  - **Deliverable:** Integrated quizzes and interactive features that function correctly across devices.

- Week 5-6: Initial evaluation and testing

  - **Deliverable:** Report summarizing initial usability testing results, identifying key issues and areas for improvements

- Week 7-9: final implementation and improvements to cybersecurity website

  - **Deliverable:** A polished, fully functional website with improvements based on evaluation feedback, optimized for all devices

- Week 9: evaluation experiments run

  - **Deliverable**: Comprehensive evaluation report based on user feedback and testing data from a larger group of users.

- Week 8-10: Write up

  - **Deliverable**: first draft submitted to supervisor two weeks before final deadline