Personal Development Report (PDR)

Student Name: Bruno Carvalho
Date: 16-03-2025
Course: AI for Society Minor

1. Introduction

- **Abstract**: The integration of artificial intelligence with cybersecurity presents an opportunity to enhance security awareness. This minor was chosen due to its potential to contribute to an ongoing cybersecurity awareness initiative. The project extends previous efforts to educate individuals on cybersecurity best practices, with a focus on ensuring that users understand threats and take actionable steps to secure their digital environments. The AI-powered cybersecurity assistant aims to bridge the knowledge gap by providing accessible, personalized security recommendations.

Research Question: How can AI be leveraged to enhance cybersecurity awareness and improve individual security behaviors?

Sub-Research Questions:

- What are the primary barriers preventing individuals from engaging in proactive cybersecurity measures?
- How can AI models be trained to deliver tailored security advice based on user knowledge levels?
- What visualization techniques improve user engagement with cybersecurity recommendations?

Technologies and Methods: The project will utilize large language models (LLMs), survey-based insights, and interactive visualizations to provide cybersecurity guidance.

2. Learning Outcome Evaluations

Each section follows this structure:
(a) Explanation of the Learning Outcome
(b) Self-Assessment & Current Progress
(c) Learning Process & Evidence (Feedback, research, datasets, initial models, survey results, etc.)
(d) Reflection & Next Steps

2.1 LO1 - Societal Impact

- **Explanation**: Enhancing cybersecurity awareness and promoting proactive security behaviors among users.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**: Research on user engagement with cybersecurity, psychological barriers to adoption, and effectiveness of digital education tools.
- **Reflection & Next Steps**: Incorporate survey findings to identify key behavioral patterns and refine the assistant's educational approach.

2.2 LO2 - Investigative Problem Solving

- **Explanation**: Addressing the challenges in cybersecurity awareness and proposing AI-driven solutions.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**: Analysis of gaps in existing cybersecurity training, initial review of AI-based educational tools.
- **Reflection & Next Steps**: Evaluate AI-driven methodologies for adaptive learning and engagement.

2.3 LO3 - Data Preparation

- **Explanation**: Collecting and refining data sources to enhance model training and cybersecurity insights.
- **Self-Assessment**: Beginning.
- **Learning Process & Evidence**:
    - Identified datasets (MITRE ATT&CK, OWASP, etc.).
    - Survey responses (213 responses), capturing user behaviors and perceptions of cybersecurity.
    - Dataset sources (Google Dataset Search).
    - Preliminary analysis of survey data, identifying trends in security practices.
- **Reflection & Next Steps**: Process and clean data for model training, expand dataset diversity.

2.4 LO4 - Machine Teaching

- **Explanation**: Training an AI model to generate cybersecurity insights in an accessible manner.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**:
  - Initial exploration of fine-tuning LLMs for educational purposes.
  - Review of GPT-3.5, Llama, and BERT applications in cybersecurity education.
- **Reflection & Next Steps**: Determine optimal model structure and initial testing environment.

2.5 LO5 - Data Visualization

- **Explanation**: Enhancing cybersecurity learning through interactive and visual representations.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**:
  - Review of visualization techniques (decision trees, checklists, interactive dashboards).
  - Preliminary survey analysis with graphical representation.
- **Reflection & Next Steps**: Select visualization tools and frameworks for the AI assistant.

2.6 LO6 - Reporting

- **Explanation**: Documenting research findings, methodology, and results.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**:
  - Developed Personal Challenge Proposal.
  - Collected initial feedback from mentors and contextual consultants.
- **Reflection & Next Steps**: Refine reporting structure, integrate ongoing feedback.

2.7 LO7 - Personal Leadership

- **Explanation**: Developing initiative and leadership within AI and cybersecurity.
- **Self-Assessment**: Orienting.
- **Learning Process & Evidence**:
  - Management of project milestones and coordination of research efforts.
- **Reflection & Next Steps**: Strengthen strategic decision-making and technical implementation skills.

2.8 LO8 - Personal Goal

- **Explanation**: Gaining AI expertise in the context of cybersecurity.
- **Self-Assessment**: Orienting.

- **Learning Process & Evidence**: Structured project planning, application of AI methodologies.
- **Reflection & Next Steps**: Implement iterative improvements based on feedback and performance evaluation.

3. Retrospect (Final Submission Only)

- **Course Experience**: Analysis of AI for Society minor's impact on skill development.
- **Challenges & Improvements**: Review of project difficulties and areas for enhancement.
- **Future Applications**: Exploration of long-term applications of AI in cybersecurity.

4. Conclusion (Final Submission Only)

- **Success Assessment**: Justification of learning outcomes achieved and project impact.

5. Appendices

- **Relevant references, datasets, survey results, consultant feedback screenshots, etc.**