1. Research and Data Collection
   1. Gather existing datasets of labeled phishing domains
   2. Research latest AI/ML techniques for domain classification
   3. Identify relevant features for phishing domain detection
2. Data Preprocessing and Feature Engineering
   1. Data cleaning and preprocessing
   2. Feature selection and extraction
3. Model Development and Training
   1. Select appropriate AI/ML algorithms (e.g., Random Forest, SVM)
   2. Split data into training and testing sets
   3. Train initial models
4. Model Evaluation and Validation
   1. Evaluate models using performance metrics (e.g., accuracy, precision, recall)
   2. Validate models using cross-validation techniques
   3. Fine-tune hyperparameters
5. Deployment and Testing
   1. Integrate model into a user-friendly tool
   2. Test tool with sample phishing domains
   3. Gather feedback and make necessary improvements

Monthly Schedule:

Month 1: Work Package 1

Month 2: Work Package 2

Month 3: Work Package 3

Month 4: Work Package 4

Month 5: Work Package 5