



AI User Safety Application

Project Advisor: Professor Vijay Eranti

Team Members: Gulnara Timokhina

Mirsaeid Abolghasemi

Varun Bhaseen



Project Description

- Protect users and their private data from phishing attacks on a web page.
- A real time Natural Language Processing (NLP) and Computer Vision (CV) based agent as a plugin to scan web page for phishing attack in a web browser.
- Plugin will display notifications and alerts for malicious scripts, phishing intent, inaccurate domain address and finding discrepancies in logos and images.



Project Deliverables

- A final plugin package for a web browser.
- Datasets used for Deep Learning model training.
- Colab notebook files with solutions using Deep Learning model.
- Github source code for the project.
- A research paper comprising of the solution and approach.



Project Dependencies and Concerns

- Research on working (and limitations) of plugins.
- Gathering and preprocessing of data/datasets.
- Fine tuning of model to give accurate results.
- Finding state of the art deep learning models for the problem statement.
- A reliable database for validating network domain address.
- Combining a natural language processing and computer vision model together as a web plugin.