# **Detailed Project Proposal**

|  |  |
| --- | --- |
| First Name: | Navya |
| Last Name: | Shiju |
| Student Number: | 1903940 |
| Supervisor: | Mark Zarb |

## **Defining your Project**

**1.1 Project title**

***Help:*** *a brief statement about what you are going to do.*

|  |
| --- |
| **Phishing URL Detection using Machine Learning Models** |

**1.2 Background**

***Help:*** *Provide the background to your project. This section should highlight the main topics in the area you are going to research. Essentially what is the project about, what has been done before and why is this project important? ~500 words*

|  |
| --- |
| Phishing attacks are a prevalent and growing threat in the digital space, where attackers mislead users into providing private information by presenting themselves as reliable entities. One of the most common methods of phishing involves the using deceptive URLs, that appear legitimate but lead to malicious websites. Detecting these phishing URLs is crucial for protecting users and organizations from data breaches, financial loss, and other cyber threats.  Phishing URL detection using machine learning has become a promising approach to address this challenge. Machine learning models can analyze various features of URLs such as domain information, length of link, etc. to distinguish between legitimate and phishing URLs. This project aims to make use of machine learning models to enhance the accuracy and efficiency of phishing URL detection and develop a feature that allows a potentially malicious URL to be entered and a response to be given in real-time as to whether it is malicious or genuine.  Numerous studies have explored different machine learning models and techniques for phishing URL detection. For instance, researchers have used deep learning models, such as Convolutional Neural Networks (CNNs), to achieve fast and accurate detection using URL features. (Siddiq et al., 2022).Other methods have applied supervised machine learning algorithms, including Decision Trees, Random Forests, and Support Vector Machines (SVMs), to classify URLs based on a variety of features.(Mahajan et al., 2018).  The importance of this project cannot be understated – and that knowledge was further cemented during my year-long industrial placement within the Cyber Security team at a large, international company, at which I still work at today. The significance the team, and the company, placed on educating its’ users taught me that, no matter what software and procedures a company has in place to protect its firewalls and gateways, the last line of defence is the end user, and human error plays a large factor in the number of incidences that can affect a company. “Researchers from Stanford University and a top cybersecurity organization found that approximately 88 percent of all data breaches are caused by an employee mistake. Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems.” - (Sjouwerman, 2024).  Currently, most companies use a dedicated security operations team to analyse any potential phishing emails that get reported by an employee and provide them with a verdict of their authenticity – however, there can be a noticeable time delay in responses, especially when taking into consideration the number of queries that get brought forth within a large company. One of the practical benefits of this project is the speed at which an answer can be provided to a user – decreasing the likelihood of a user falling to temptation and proceeding to interact with the link anyway. If an employee can be aided by even a small degree with the practical applications of this project, it will prove to significantly impact the security posture of a given company.  References:   * Sjouwerman, S. (2024) *Stanford Research: 88% of data breaches are caused by human error*, *KnowBe4 Security Awareness Training Blog*. Available at: https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error#:~:text=Researchers%20from%20Stanford%20University%20and,overwhelming%20majority%20of%20cybersecurity%20problems. (Accessed: 03 October 2024). * Siddiq, Md.A., Arifuzzaman, M. and Islam, M.S. (2022) ‘Phishing website detection using Deep Learning’, *Proceedings of the 2nd International Conference on Computing Advancements*, 2019, pp. 83–88. doi:10.1145/3542954.3542967. * Mahajan, R. and Siddavatam, I., 2018. Phishing website detection using machine learning algorithms. *International Journal of Computer Applications*, *181*(23), pp.45-47. |

**1.3 Aim & Objectives**

***Help:*** *Outline what are the main things your project is going to do and what steps or milestones will be used to achieve this aim. The Aim is unlikely to change throughout your project; however, the objectives are likely to adapt to your ongoing research and development.*

**Example**:

Aim: To create a functioning attendance application that efficiently automates the taking of class registers.

Objective 1: Study existing register system in place at RGU and identify weaknesses

Objective 2: Research existing automation technology’s and identify and evaluate those that may be appropriate to taking in class registers

Objective 3: Implement chosen technologies to create prototype application

Objective 4: Conduct user trials to evaluate capabilities of prototype application

Objective 5: Create a refined application incorporating feedback from user trials

|  |
| --- |
| **Aim:** To detect phishing URLs by analysing numerous features embedded within the links that separate malicious websites from the genuine by creating various machine learning models and comparing their performance and accuracy.  **Objective 1:** Review existing research on the benefits of Phishing URL detection and the practical benefits and capabilities it offers large corporations.  **Objective 2:** Conduct an extensive review of the existing literature to determine which Machine Learning models are ideally suited to Phishing URL analysis.  **Objective 3:** Identify and extract key features from URLs within the dataset that are indicative of phishing attempts.  **Objective 4:** Implement and train three Machine Learning models using the identified features.  **Objective 5:** Evaluate the performance of the trained models using appropriate metrics such as accuracy, precision, F1-score, etc. and proceed to tune and improve further.  --------------------------------------------------------------------------------------------------------  **Objective 6:** Develop a prototype feature within Google Colab file that utilizes the best-performing model to detect phishing URLs in real-time. |

**1.4 Tools & Technologies**

***Help:*** *Perform some initial research into the area and outline what tools and techniques you expect to be using in your project.*

|  |
| --- |
| **Tools -**   * Google Colab   **Techniques –**   * Various Machine Learning models – to be specified and narrowed down after initial research - most likely to include Random Forest and Decision Tree. |

**1.5 Project Plan**

***Help:*** *This is the project plan as to how you will go about achieving your objectives over the timescale of the Honours Project. At a minimum this can be a month-by-month plan.*

|  |
| --- |
| **October –**  **Week 1 (1/10/24 - 6/10/24):**   * Initial background research on various machine learning models that are best suited for Phishing URL datasets, the importance of Phishing prevention as it pertains to large organisations, what has been done previously in the field * Submit Project Proposal + Ethics Form on the 3rd October 2024 * Start extensive review of existing literature within Google Scholar and gathering of initial sources   **Week 2 (7/10/24 – 13/10/24):**   * Continue extensive research, collate sources together, draft outline of the project scope * Proceed to write the Project Scope   **Week 3 (14/10/24 – 20/10/24):**   * Finalise 1st draft of the Project Scope * Submit Project Scope to supervisor for feedback   **Week 4 (21/10/24 – 27/10/24):**   * Make adjustments/improvements to Project Scope based on feedback received from supervisor * Finalise Project Scope submission in terms of proof-reading, references, formatting, etc.   **Week 5 (28/10/24 – 31/10/24):**   * Submit Project Scope   **November –**  **Week 1 (1/11/24 – 3/11/24):**   * Initial set up of Google Colab file   **Week 2 (4/11/24 – 10/11/24):**   * Import required libraries * Start the Data Processing Stage – this will involve cleaning and labelling raw data that is appropriate for machine learning algorithms and then exploring and visualising the data   **Week 3 (11/11/24 – 17/11/24):**   * Continue processing data   **Week 4 (18/11/24 – 24/11/24):**   * Continue processing data   **Week 5 (25/11/24 – 30/11/24):**   * Finish processing the data – log/record all advancements made/challenges experienced in this phase and start populating the report template   **January –**  **Week 1 (1/1/25 – 5/1/25):**   * Start the Model Development Stage – this will involve splitting the data into training and test sets, creating the three models, evaluating their performance, and then tuning them further. Ensure a constant loop of conversation with the supervisor in this time period to ensure that everything remains on track.   **Week 2 (6/1/25 – 12/1/25):**   * Continue developing models   **Week 3 (13/1/25 – 19/1/25):**   * Continue developing models   **Week 4 (20/1/25 – 26/1/25):**   * Continue developing models   **Week 5 (27/1/25 – 31/1/25):**   * Continue developing models – log/record all advancements made/challenges experienced in this phase and start populating the report template   **February –**  **Week 1 (1/2/25 – 2/2/25):**   * Start evaluating the performance of the trained models using appropriate metrics and tuning them for better results. Ensure a constant loop of conversation with the supervisor in this time period to ensure that everything remains on track.   **Week 2 (3/2/25 – 9/2/25):**   * Continue evaluating and improving   **Week 3 (10/2/25 – 16/2/25):**   * Continue evaluating and improving   **Week 4 (17/2/25 – 23/2/25):**   * Continue evaluating and improving   **Week 5(24/2/25 – 28/2/25):**   * Continue evaluating and improving until the models reach very high accuracy results – log/record all advancements made/challenges experienced in this phase and start populating the report template   **March –**  **Week 1 (1/3/25 – 2/3/25):**   * Develop a prototype feature within Google Colab file that utilizes the best-performing model to detect phishing URLs in real-time. Ensure a constant loop of conversation with the supervisor in this time period to ensure that everything remains on track.   **Week 2 (3/325 – 9/3/25):**   * Continue development and debugging   **Week 3 (10/3/25 – 16/3/25):**   * Continue development and debugging   **Week 4 (17/3/25 – 23/3/25):**   * Continue development and debugging   **Week 5 (24/3/25 – 30/3/25):**   * Continue development and debugging   **Week 6 (31/3/25):**   * Finish developing the feature that allows phishing URLs to be analysed in real-time and thoroughly test it against various possible inputs– log/record all advancements made/challenges experienced in this phase and start populating the report template   **April –**  **Week 1 (1/4/25 – 6/4/25):**   * Start the reminder of the write up – ensure a constant loop of conversation with the supervisor in this time period to ensure that everything remains on track   **Week 2 (7/4/25 – 13/4/25):**   * Continue the write up   **Week 3 (14/4/25 – 20/4/25):**   * Finish the write up and proofread fully   **Week 4 (21/4/25 – 27/4/25):**   * Submit final deliverable   **May –**   * Present at Degree Show |

**1.6 Ethics Form**

***You must include in your signed ethics form in this submission, or you will not be able to continue the project.***