**Capstone Project Proposal Report**

**(Individual Report)**

**Instructions:**

This form is to be completed by each student doing Project registration to fulfill their senior design or capstone requirement. It must be completed and submitted to your Guide. Each student must complete this form individually.

This report is to be completed during the starting of the semester, while the project description report will be completed during the end of the semester.

|  |  |  |
| --- | --- | --- |
| Guide Approval (initials/date): |  |  |

**CAP4001– Capstone Project Proposal Report**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student Name** | | **Harrison Korodi** | | |
| **Student Register Number** | | **15BCN4002** | | |
| **Program** | | Cyber Security & Network Technology | | |
| **Semester/Year** | | 6th Semester | | |
| **Guide(s)** | | Prof. Bob Hayton | | |
| **Project Title** | | Phishing Detection: Using Machine Learning | | |
|  | | | | |
| **Reg. No** | **Name** | | **Major** | **Specialization** |
| 15BCN4002 | Harrison Korodi | | Cyber Security | Network Technology |

**Project and Task Description**: Provide a brief (one or two page) technical description of the design project and your specific tasks, as outlined below: (use a separate sheet)

1. Provide a summary of the project, including a description of the project and its requirements, the purpose, specifications, and a summary of the approach. If this is a continuing project, you may use and/or edit the same project description.
2. Describe the specific role and tasks that **you individually** will be completing as part of the design of the project. What **specific deliverables** will you produce?
3. Discuss in detail the specific approach that will be used to complete **your** portion of the design.
4. Describe the phases of the design process that will be incorporated and what work will be accomplished during those phases. (you may attach a Gantt Chart)

**Outcome Matrix:** Describe your plan to demonstrate each of the outcomes below.

|  |  |
| --- | --- |
| **Outcomes:** | **Plan for demonstrating outcome:** |
| a) an ability to apply knowledge of mathematics, science, and engineering | The following will be accomplished by performing data analysis and designing and implementing appropriate algorithms to achieve the project's end result. |
| b) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability | The following will be accomplished by the entire project because it focuses on a real-world problem that takes into account all of the real-world constraints that an attacker and defender would face in the industry. |
| c) an ability to communicate effectively | This outcome will be achieved throughout the project because research requires communicating with users both online and in person; communicating with the guide to resolve issues and get guidance; and presenting the project's final outcome. |
| d) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice | Machine learning and social engineering are modern-day attacker's toolkits that will be extensively used for research and implementation purposes throughout the project. |

**Realistic Constraints:**

Since phishing attacks are all user-dependent, any research conducted will be on live users with their permission. To ensure the results are authentic, detection algorithms will be ran on live datasets or logs from where the phishing attack occurred.

**Engineering Standards:**

The NIST Cybersecurity Framework is the engineering standards that will be followed throughout the project. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF) "provides a high level taxonomy of cybersecurity outcomes as well as a methodology to assess and manage those outcomes." It is intended to provide guidance to private sector organizations that provide critical infrastructure on how to protect it, as well as relevant privacy and civil liberties protections. It offers IT security advice, risk management guidelines for industries, and digital identity guidelines. Governments and industries around the world adhere to this framework.