**Major Modules**

Following are the major modules aimed to be completed in the FYP Part 1 and 2:

* Authentication & User Management System:

The authentication and segregation interface & mechanism to verify and then grant access to their relevant role functionalities/privileges. It will also provide new users with the ability to register themselves in the database or change credentials if need be. The module would also implement input validation and other preventives to safeguard the system from multiple unauthorized access techniques.

Secure login and registration system with role-based access control (RBAC) to ensure authorized access. Integration with Google reCAPTCHA for bot prevention and multi-factor authentication (MFA) for enhanced security. All while only giving them user-based functionalities and their roles and responsibilities.

* Dashboards:

The Landing Page of the whole system providing a quick overview of the company’s analytics and user performances. Along with key functionalities that would later be expanded into separate modules on single clicks. It would also give alerts and inbox for shared communication platform for certain admin and IT roles.

Developing the in-depth user dashboards for all key user profiles with each with their role-based functionalities that later be further divided into segregated functionalities and later on broken into subsequent functionality operations and subpages.

* Phishing Campaign:

The actual Test Range for the employees of the company, granting a multitude of tools and to bespoke-make scenarios and situations reflecting the current threat landscape in the industry. It would also provide quality of life features like scheduling, auto listing candidates for such campaigns by automated evaluation of user performances stored in the database.

Allows administrators to create, customize, and schedule phishing campaigns. Includes email template management, campaign tracking, and automation for efficient campaign execution.

* Notification Mechanism**:**

Proper notification and system be enforced while having a meticulous email builder going hand in hand with the phishing email template engine for forwarding the phishing attempts.

* User - Reporting & Analytics Portal:

Generate detailed phishing campaign reports with real-time insights. Provides metrics on user interactions, email open rates, link clicks, and form submissions, helping organizations assess employee security awareness.

This module will list users and all their respective fields like certifications, calibre, test scores, training progress, rankings and performances. Moreover, this module would give a meticulous display of the overall company’s standing chronologically. The relevant authorities would be notified by the system after each major event closes while giving them the ability to download all this data into PDFs for documentation and governance purposes.

This would be responsible for the progress tracking, numbers generation and overall company evaluation. Through automated tracking techniques and procedures at the back-end.

* Database & Backend:

Secure and seamless integration of the front and back end with detailed and reliable databases for each key storage functionality. After being ensured through our agile testing and Quality Assurance practices. While using certain APIs for the back-end connectivity.

* Phishing Campaign:

Evaluation through rigorous test runs, incorporating both automated (if need be) and manual **Quality Assurance (QA) and Quality Control (QC)** mechanisms. The evaluation process will focus on functionality, security, usability, and performance to ensure that PhishNet meets industry standards and user expectations. With the use of Automated Testing, Manual Testing, End User Experience, Self Simulations. Unit Integration.

* Debugging & Improvements:

Rectifying our project’s setbacks and patching the issues via refinements and debugging again and again. While also introducing quality of life improvements to the overall project’s fine working and everyday experience.

* Evaluation Mechanism:

The evaluation and rewarding aspect of the solution, granting badges and certification to the users on passing each test or training phase to better evaluate the company standing with regards to market threats. While helping improve the match making system for future phishing and training campaigns.