The project "Phishing Website Detection" focuses on developing advanced machine learning models to effectively identify phishing websites, a significant cybersecurity threat. Phishing attacks, which involve deceiving users into revealing sensitive information, have become increasingly sophisticated, and traditional detection methods often fail to keep pace with these evolving tactics. The project's primary objective is to create a robust system that can accurately distinguish between legitimate and malicious websites, protecting users from financial fraud, identity theft, and other cybercrimes.

By utilizing various URL-based features such as IP address, domain age, page rank, and WHOIS information, alongside modern machine learning, deep learning techniques, and Large Language Models (LLMs), the system aims to enhance the detection of both known and unknown phishing attempts. This approach ensures adaptability and efficiency, reducing false positives and negatives, and strengthening the overall cybersecurity environment. The integration of AI-based techniques with feature engineering promises to improve real-time detection, providing a powerful tool against phishing attacks while safeguarding digital ecosystems.