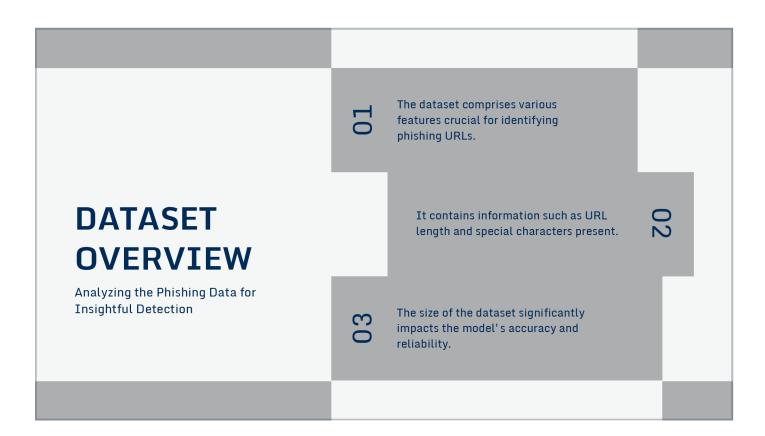
	01	Phishing is a fraudulent attempt to obtain sensitive information.		
Introduction to Phishing		Over 90% of cyberattacks start with phishing, making it crucial to address.	02	
Understanding phishing and its significant impact on cybersecurity.	03	Awareness and education are essential in combating this growing threat.		

	01	Phishing websites are growing rapidly , targeting unsuspecting users online.		
Phishing Threats		Traditional blacklisting methods are ineffective against new and evolving phishing tactics.	02	
Understanding the increasing danger of phishing websites today.	03	An intelligent detection system is essential for real-time protection against these threats.		

	01	Our goal is to accurately classify URLs as phishing or legitimate .		
Objective Developing a Machine Learning-Based Detection Tool		The tool relies on feature-based analysis rather than static rules for classification.	02	
	03	This approach enhances detection capabilities and provides real-time results for users.		

	01	The backend is built using Python and Flask for efficient processing.	
Technology Stack		Machine learning is implemented with Scikit-learn, specifically using the Random Forest algorithm.	03
Overview of tools and technologies used in the project.	03	The frontend utilizes HTML along with Flask templates for dynamic content rendering.	



	01	Key features include URL length and presence of HTTPS.	
Feature Extraction		Suspicious keywords and special characters play a significant role.	02
Identifying crucial aspects for effective phishing detection.	03	These features enhance the model's ability to classify URLs accurately.	

	01	The Random Forest Classifier was utilized for its accuracy and efficiency.		
Model Training		An 80/20 train/test split ensured effective model evaluation and performance assessment.	02	
Building a robust classification model for phishing detection.	03	The model was serialized using joblib to facilitate real-time predictions in deployment.		

	01	Users submit URLs through a simple web form.		
Application Flow		The system processes the URL and extracts relevant features.	02	
User interaction process for detecting phishing URLs	03	Finally, the model classifies the URL as 'Phishing' or 'Legitimate'.		

	01	Corporate firewalls can effectively utilize this tool for enhanced security.		
Real-World Applications		Email gateways benefit from real-time phishing URL detection to protect users.	02	
Exploring practical uses of the phishing detection tool.	03	Web browser plugins can provide users with immediate alerts on suspicious links.		

	01	Integrating deep learning could improve detection accuracy significantly.		
Future Enhancements		Adding live web scrapers would enhance real- time URL analysis capabilities.	02	
Expanding the Tool's Capabilities for Better Detection	03	Developing a browser extension would allow for seamless user protection.		

	01	Generalizing features was difficult for unknown phishing types.		
Challenges Faced		We faced inconsistencies within the dataset that needed addressing.	02	
Overcoming obstacles in developing our detection system	03	Ensuring fast predictions with Flask was a significant challenge.		

	01	The project successfully built a highly accurate phishing URL detection system.		
Achievements Summary of accomplishments and future development directions		Future enhancements will focus on integrating deep learning and advanced features.	02	
	03	This scalable solution holds significant potential for improving cybersecurity measures .		

"A game changer in phishing detection and prevention!"

- Mark Thompson

"This tool significantly improved our cybersecurity measures."

- Sarah Jenkins

"Impressive accuracy and usability for real-time applications."

– Lisa Wong

"A vital resource for modern cybersecurity challenges."

– Raj Patel