# *PRESENTATION:*

*Email Phishing Detector using Machine Learning*

*Submitted by:* Pralabh Kushwaha

*Team Name:* REDVENOM

*Organized by:* Digisuraksha Parhari Foundation *Powered by:* Infinisec Technologies Pvt. Ltd.

## Slide 1: Title Slide

*Project Title:* Email Phishing Detector using Machine Learning *Intern:* Pralabh Kushwaha *Team:* REDVENOM

## Slide 2: Introduction

- Email phishing is a major cybersecurity threat.
- Attackers trick users via emails to steal data.
- Traditional spam filters are not enough.

## Slide 3: Problem Statement

- Email phishing causes identity theft, fraud, and data breaches.
- Increasingly sophisticated and harder to detect.
- Need for an intelligent, automated detection system.

## Slide 4: Objectives

- Detect phishing emails using ML & NLP.
- Build a real-time tool with GUI.
- Evaluate email content and give security suggestions.

## Slide 5: Literature Review

- Past research used decision trees, SVM, and blacklists.
- Lacked real-time capability and semantic analysis.
- Our tool improves on those using TF-IDF + Logistic Regression.

## Slide 6: Methodology

- Data Collection: Phishing & legitimate emails from Kaggle.
- Preprocessing: Tokenizing, cleaning, stemming.
- Feature Extraction: TF-IDF.
- Model: Logistic Regression.
- GUI: Built with Streamlit.

## Slide 7: Tool Overview

- Input: Email content in text format.
- Output: Prediction – Phishing or Legitimate.
- Also shows risk level and suggestions.

## Slide 8: Implementation Details

- Python libraries: scikit-learn, nltk, pandas, streamlit.
- Accuracy achieved: 95.3%.
- Real-time processing and lightweight GUI.

## Slide 9: Results & Evaluation

- Accuracy: 95.3%
- Precision: 94.8%
- Recall: 93.7%
- F1-score: 94.2%
- Effective on both standard and obfuscated phishing emails.

## Slide 10: Ethical Impact

- Promotes secure digital behavior.
- No user data stored or shared.
- Designed only for defense and education.

## Slide 11: Market Relevance

- Useful for email providers, corporates, and end users.
- Easily integrable into security suites.
- High demand for automated phishing filters.

## Slide 12: Future Scope

- Add URL/attachment/header analysis.
- Use LSTM/BERT for deep semantic understanding.
- Deploy as browser plugin or cloud API.

## Slide 13: Conclusion

- Project successfully built a phishing detection system.
- Helps users avoid scams and stay safe online.
- Contributes to national digital security.

## Slide 14: Thank You

*Questions?* Email: kushwahapralabh@gmail.com

GitHub: https://github.com/pralabhkushwaha/pralabhkushwaha