Market Analysis: AI-Powered Phishing Email Detection

1. Market Need

Phishing attacks continue to be one of the most successful forms of cybercrime. According to reports by Verizon and IBM, over 90% of cyberattacks begin with phishing emails. Organizations globally are investing heavily in phishing detection, email security gateways, and AI-based threat intelligence to protect their data and users.

2. Target Audience

The target audience for an AI-Powered Phishing Detector includes:

- Small to medium businesses lacking dedicated cybersecurity teams
- Educational institutions and universities
- Email service providers
- Enterprises looking to enhance employee email security
- Individual users and freelancers

3. Existing Solutions

Current tools in the market include Microsoft Defender for Office 365, Proofpoint, Mimecast, and Barracuda. These tools often integrate with enterprise mail servers and use a combination of heuristics, ML models, and blacklists. However, many of them are costly or not tailored for individual or academic users.

4. Competitive Advantage

This project offers:

- An open-source, lightweight alternative
- Easy-to-use CLI and GUI for broader accessibility
- TF-IDF + Random Forest for high interpretability and low compute needs

- Extendable architecture for future deep learning enhancements

5. Market Growth Potential

The global email security market is projected to grow from $4.48 billion in 2022 to over $9 billion by 2030, driven by the rise in remote work and digital communication. AI-powered solutions are expected to dominate this growth due to their adaptability and scalability.

6. Conclusion

AI-Powered Phishing Detection is a timely and relevant cybersecurity solution. With its educational value, practical implementation, and adaptability, this tool has real-world market relevance in both enterprise and academic environments.