inQueries: An Explainable RAG-AI Chatbot for Scam Link Detection in Messaging Platforms

1. Executive Summary

inQueries is a lightweight, AI-powered Telegram chatbot that detects scam links and explains risks in real time using a retrieval-augmented generation (RAG) framework. It integrates open-source tools, local large language models (LLMs), and threat intelligence APIs to deliver fast, explainable, and accessible security alerts. Designed for non-technical users and small organizations, *inQueries* addresses phishing in messaging platforms—an increasingly common attack vector.

2. Market Analysis

Target Users:	Competitors:
• General users of Telegram/WhatsApp • Small businesses and NGOs with limited cybersecurity capacity • Cybersecurity educators, digital literacy programs • Public awareness campaigns (government/NGO)	• Basic Telegram spam bots • Commercial phishing tools (e.g., Proofpoint, Cofense) • Generic LLM bots (e.g., ChatGPT) without integrated scanning

3. Problem Statement

Users increasingly receive scam links through private messages. Yet most phishing detection tools are:

- Designed for enterprise use, not public platforms
- Focused on binary decisions without explanations
- Not integrated into real-time messaging workflows

Users need tools that are simple, explainable, and embedded within the apps they already use.

4. Unique Value Proposition

"*Real-time, explainable phishing detection in your chat – powered by AI, built for humans.*"

- Works inside Telegram via chatbot
- Provides structured, human-readable summaries, not just alerts
- Operates entirely on free-tier, open-source tools
- Designed with privacy and simplicity in mind

5. Objectives

- Deploy a working prototype for public use on Telegram
- Deliver fast and accurate scam detection using local models
- Convert threat data into readable, confidence-based summaries

- Evaluate system responsiveness and usability

6. Methods and Scope

Methods:

- Real-time data from VirusTotal + urlscan.io
- Vector retrieval via Pinecone
- LLM summarization (LLaMA 3.2 via Ollama)
- Built using n8n, Docker, and Telegram API

Scope:

- Supports URL-based phishing inside Telegram
- No file-based malware or deep content parsing
- Manual prompt-based summarization (no fine-tuning)

7. Business Model

- **Freemium** approach
- Free for public; paid plans for SMEs with logs, dashboard, and priority support
- Projected break-even with ~50 monthly SME users
- Very low operating cost due to use of free-tier services

8. Milestones and Key Metrics

Milestone	Timeline
Public bot launch (Telegram)	Month 1
Feedback buttons integration	Month 2
SME pilot with usage analytics	Month 3–4
Prompt refinement & dashboard	Month 5–6

Key metrics: user count, response latency, explanation clarity rating

9. Project Outcome

- A functioning proof-of-concept chatbot
- Real-time threat alerts with explainability
- Demonstrates potential for public cybersecurity applications
- Fully reproducible, modular, and privacy-conscious architecture

10. SWOT Analysis

Strengths	Weaknesses
Works inside real chat interface	Limited to URL-based detection
Explainable, LLM-powered output	Manual prompt engineering only
Zero-cost architecture	Relies on free-tier API quotas

Opportunities	Threats
Expanding phishing via messaging	Competing bots or platform features
Digital literacy and education	Public trust in AI security tools