P.I.S.H

(Phishing Intelligence & Security Hub)

1) Introduction

P.I.S.H(Phishing Intelligence & Security Hub) is a real-time AI/ML-powered phishing detection and prevention system designed to protect users from modern cyber threats across three major channels: **WhatsApp messages, voice calls (vishing), and emails**.

As phishing has become more sophisticated—leveraging impersonation, fraudulent identities, fake bank notices, and deceptive communication—users increasingly require a smart system that can identify risks instantly and guide them safely.

Distil BERT-based NLP, heuristic analysis, sender reputation scoring, and automated device-level defence mechanisms such as **hotspot isolation** to detect and prevent phishing attempts with high accuracy and low latency.
Its goal is to provide **immediate protection**, **user awareness**, and **practical actions** to reduce financial losses and scam success rates.

---

2) Problem Statement (PS)

P.I.S.H is the most common cyberattack today, exploiting human psychology instead of technical vulnerabilities. Attackers use:

- Fake WhatsApp messages posing as banks, police, or government officials
- Voice call impersonation using spoofed names and caller IDs
- Fraud emails claiming suspicious activity, KYC updates, payments, and job offers

Most users **cannot distinguish** between legitimate and fraudulent communication.
Traditional security tools fail because:

- They do not analyse **real-time conversational messages**
- They cannot detect **social engineering tone or urgency**
- They cannot respond automatically (like isolating hotspot)
- They do not educate users during an attack

Therefore, there is an urgent need for a **real-time, multi-channel, AI-powered detection system**.

---

3) Problem Solution

P.I.S.H solves the problem by providing **continuous monitoring + instant AI-powered threat detection + automated prevention** across WhatsApp, calls, and emails.

Key solution strategies include:

A) AI-Based Text Understanding (Distil BERT NLP Model)

Uses transformer language models to identify phishing intent, urgency, financial manipulation, fake threats, and malicious URLs

B) Behavioural & Heuristic Analysis

- Detects common scam patterns
- Identifies impersonation attempts
- Flags unknown or high-risk senders

C) Real-Time Alerts with Actionable Guidance

Users receive popups explaining:

- Why the message/call/email is risky
- What immediate steps they should take
- How to report the scam
- Government cyber helpline details

D) Automated Protection (Hotspot Isolation)

If a fraud caller tries to socially engineer a user and hotspot is ON, P.I.S.H automatically **turns OFF the hotspot** to prevent remote hacking/connection attempts.

E) Scoring System with Severity Levels

Safe / Suspicious / High-Risk classification based on ML model + heuristics.

F) Dashboard & Logs for Pro Users

Shows threats blocked, history, WhatsApp messages scanned, security score, etc.

---

4) Products Overview

P.I.S.H provides **three core detection products**, each targeting a major phishing channel.

4.1 WhatsApp Phishing Detection

Purpose

Detect fraudulent text messages, malicious links, impersonation messages, lottery scams, job frauds, banking/KYC scams, etc.
When suspicious content appears, P.I.S.H immediately displays a popup warning.

How It Works

✓ Extracts message text → Preprocesses → Runs through Distil BERT → Calculates phishing score
✓ Cross-checks sender reputation
✓ Detects urgency phrases, fake authority language, scam keywords
✓ Shows threat warning + recommended actions

User Actions Provided

- Ignore the message
- Report to cybercrime
- Read awareness tip
- Call helpline 1930

Impact

Helps reduce accidental link clicks, OTP sharing, and fraud losses.

4.2 Vishing Detection & Auto Isolation

Purpose

Detect fraudulent phone calls where attackers impersonate:

- Banks
- Police departments
- Income tax
- Delivery companies
- Telecom operators

How It Works

✓ Analyses caller metadata and patterns
✓ Detects spoofed caller names
✓ Flags impersonation attempts
✓ Shows a threat popup instantly

Auto-Isolation Feature

If hotspot is ON and the call appears malicious:
➞ **P.I.S.H automatically disables the hotspot** to block potential device infiltration.
This is a unique and innovative security feature.

User Options

- Hang up
- Report number
- View safety guidance

- Call cyber helpline

4.3 Email Phishing Detection

Purpose

Detect phishing emails with fraudulent senders, fake invoices, malicious links, and social-engineering content.

How It Works

✓ Extracts subject + body + URLs + sender details
✓ Runs ML classification and heuristics
✓ Checks domain reputation, redirections, DKIM/SPF patterns
✓ Shows phishing score popup
✓ Offers email quarantine to isolate harmful mail

Capabilities

- Detects credential harvesting
- Identifies job scams, refund scams, and banking scams
- Flags malware or suspicious attachments

---

5) Market Go-To Strategy and Pricing

P.I.S.H uses a **freemium + subscription + enterprise SaaS model**.

Target Market

- General smartphone users
- College students (high scam exposure)
- Working professionals
- Small businesses
- BFSI customers
- High-risk groups (elderly, online shoppers)

Go-To Market Strategy

1. **Freemium Launch**
   → Offer free basic link scanning to gain mass adoption.
2. **Awareness Marketing**
   → Cybersecurity campaigns, WhatsApp scam awareness, social media presence.
3. **Partnerships**
   → Collaborate with fintech, telecom, educational institutions, cybersecurity cells.

4. **Browser Extension Distribution**
   → Chrome Web Store, Edge Add-ons Store for instant visibility.
5. **Enterprise Licensing**
   → Provide API-based phishing detection to businesses.

Pricing Strategy (from website)

- **Free Tier:** Basic scanning, limited daily uses
- **Basic Plan:** Browser extension + history
- **Pro Plan:** WhatsApp scanning, unlimited scans, dashboard access
- **Enterprise:** Custom pricing, large-scale integrations, team dashboards

---

6) Technologies Used

P.I.S.H uses a robust modern tech stack:

AI/ML

- **Distil BERT** (primary phishing classifier)
- Logistic Regression (lightweight fallback model)
- Threat score calibration mechanisms
- Dataset of ~3,000 labelled samples (WhatsApp, email, vishing transcripts)

Backend

- **Python + Fast API** for model inference APIs
- Cloud-based deployment (AWS/Render)

Frontend

- **React.js + Tailwind CSS** for dashboard & website
- Netlify for hosting

Mobile

- Android App (Kotlin/React Native) for real-time detection & OS-level actions

Database

- MongoDB / Firebase for logs, scan history, subscription data

Browser Extension

- JavaScript URL scanner integrated with PhishScan ML APIs

Security

- TLS 1.3 encryption
- AES-256 for sensitive logs

- Privacy-by-design architecture

---

7) Conclusion

P.I.S.H provides a powerful and innovative real-time phishing protection ecosystem.
By combining **AI-driven NLP**, **behavioural analysis**, **automatic hotspot isolation**, and **multi-channel monitoring**, it addresses the gaps left by traditional antivirus tools.

Its strength lies in:

- Multi-channel coverage (WhatsApp + Calls + Email)
- Fast, lightweight Distil BERT inference
- Clear user guidance
- High accuracy phishing score
- Preventive actions, not just detection
- Scalable subscription-based model

P.I.S.H is designed to significantly reduce financial fraud, prevent identity theft, and educate users, making it a highly relevant solution in today's rapidly evolving cyber threat landscape.