Project Name: *PhishNet*

Overview

PhishNet is a hybrid, privacy-preserving cybersecurity application that leverages a lightweight local LLM for real-time scam and phishing detection on mobile and wearable devices, with cloud escalation for complex cases. Designed for the general public in **Australia** and the **USA**, it aims to provide a holistic, intelligent approach to email fraud protection.

Goals

- Real-time detection of scam, phishing, and suspicious emails.
- Use a lightweight, on-device LLM for privacy and speed.
- Escalate complex cases to a secure, cloud-hosted large model.
- Incorporate contextual, behavioral, and external threat intelligence.
- Provide educational and personal security insights for end users.

Core Features

✅ Lightweight Local Detection

- Compact transformer model (TinyLlama or DistilBERT) running on mobile/wearables using ONNX Runtime.

✅ Cloud Escalation

- Emails with ambiguous or novel language patterns are sent to a cloud-hosted LLM (e.g., GPT-4.5 or LLaMA3).

✅ Email Context Enrichment

- Adds context-specific detection rules:
    - Detects tax scams (e.g., IRS or ATO impersonations).
    - Scans for election, health, and financial relief scam language.
    - Flags spoofed domain names or delivery-based lures (Amazon, AusPost, USPS).

✅ **Personal Security Layer**

- Cross-checks business names/emails with:
  - **ABN register (Australia)**
  - **BBB or domain WHOIS (USA)**
- Verifies known businesses to catch impersonators.

✅ **Behavioral Profiling**

- Detects scams based on user habits:
  - Flags brands user never interacts with.
  - Adjusts risk level based on past behavior and region.

✅ **Dark Web Exposure Check**

- Alerts users if their credentials or email have been found in:
  - Breach databases (via APIs like HaveIBeenPwned)
  - Pastebins or known black markets.

✅ **Analytics Dashboard**

- Includes metrics like detection accuracy, false positive rates, phishing trends, and escalation frequency.

Technology Stack

Component	Tool/Library
Local Model	Hugging Face + ONNX Runtime Mobile
Cloud Backend	FastAPI, Gunicorn, PostgreSQL
Cloud Model	OpenAI API or hosted LLaMA3
Mobile UI	Flutter (cross-platform)
Analytics	Streamlit or Grafana + Prometheus
Deployment	Docker, AWS/GCP