# SCAMX — 실시간 AI 스캠 탐지 앱 | 개인 프로젝트

## 프로젝트 개요

- **프로젝트명:** ScamX
- **유형:** 개인 프로젝트
- **기여도:** 100%
- **역할:** 기획 · 풀스택 개발 · AI 파이프라인 설계 및 구현
- **기술 스택:**
  - **Backend:** Python · FastAPI · LangGraph
  - **AI/ML:** LLaMA 3.1 8B · GPT-5 Mini · Sentence Embedding
  - **Database:** PostgreSQL (NeonDB) · pgvector
  - **Frontend:** Next.js · React
  - **Mobile:** Kotlin · Android Studio

## 문제 인식

- 기존 통신사 스팸 필터는 **발신번호 기반 차단**에 국한되어, 가족·지인 사칭형 스캠 탐지 불가
- 기존 보안 앱은 **패턴 DB 매칭 방식**으로 신종 스캠 대응력 부족

## 기술 도입 및 아키텍처

LangGraph 를 활용해 **4 단계 AI 파이프라인**을 오케스트레이션하여 자동 탐지 구조 구현

1. **KOLLECTRA (경량 Transformer 분류기)**
   - 1 차 스캠 가능성 판단
   - 비스캠 메시지를 조기 차단해 LLM 호출 비용 최소화
2. **Sentence Embedding (768~1024 차원)**
   - SMS 본문을 의미 벡터로 변환
   - pgvector 코사인 유사도로 기존 스캠 패턴과 의미 비교
3. **LLaMA 3.1 8B (로컬 LLM)**
   - 벡터 유사도 기반 스캠 패턴 분석
   - 누적 데이터로 **Self-Improving 구조** 구현
4. **GPT-5 Mini (신종 스캠 전용)**
   - LLaMA 가 판단 불가한 신규 유형만 선별 호출
   - 결과를 마스킹 후 DB 저장 → 이후 LLaMA 가 처리 가능

## 개인정보 보호 설계

- 전화번호 해시 처리
- 계좌·이름 패턴 기반 마스킹
- SMS 원문 무저장 원칙
- DB 에는 **비식별 의미 데이터만 저장**하여 개인정보보호법 및 Google Play 정책 완전 준수

## 🔁 전체 파이프라인 흐름

## 성과 및 차별점

- LLM 불필요 호출 차단으로 **API 비용 약 70% 절감**
- 신종 스캠 데이터 자동 축적 구조로 **모델 재학습 없이 정확도 향상**
- Android 10+ 정책 준수 (Notification Listener 방식)
- 경찰청·공공기관 연동 가능한 **Next.js 어드민 페이지 구축**
- **고령층 친화적 UX 설계** — 알림 1 회로 위험 여부 즉시 인지 가능