ScamX – Q&A

Q1. 왜 문자 내용을 브로드캐스트로 직접 읽지 않고 알림(Notification) 방식으로 읽나요?

안드로이드 10 이후 Google 정책이 크게 바뀌면서,
통신사와 메시지 앱 사이에서 SMS 본문을 가로채는 브로드캐스트 방식이 금지되었다.
3rd-party 앱이 메시지를 먼저 읽는 구조는 개인정보보호법과 Google Play 정책 모두에 걸린다.

이 때문에 ScamX 는 정책을 우회하지 않고,
Notification Listener 기반으로 문자 본문을 읽는 방식을 선택했다.
이 방식은 정책 위반이 아니고, OEM·통신사 제한도 없으며,
Android 10+ 환경에서 가장 안정적이고 합법적인 접근 방식이다.

Q2. 문자 본문을 서버로 보내서 AI 가 분석한다면, 개인정보 문제는 어떻게 해결하나요?

ScamX 는 처음부터 **원문을 저장하지 않는 구조**를 목표로 설계했다.
이를 위해 3 단계 마스킹 파이프라인을 적용했다.

- 서버 도착 즉시 문자 원문 마스킹
- 전화번호는 해시 처리
- 계좌번호·이름 등은 패턴 기반 마스킹
- 민감 단어는 제거 또는 대체
- AI 분석 후에는 '스캠 의심', '금전 요구 패턴 감지' 같은 판단 결과만 사용자에게 전달
- DB 에는 원문이 아닌 **비식별화된 의미 벡터**만 저장
- 임베딩 테이블에도 원문이 아닌 수학적 의미 벡터만 남음

이 구조 덕분에 개인정보를 저장하지 않으면서도
AI 가 학습하고 점점 더 정확해지는 시스템을 만들 수 있었다.

Q3. ScamX 는 어떻게 사용할수록 더 똑똑해지나요?

ScamX 는 **2 단계 AI 필터 구조**를 사용한다.

1 단계는 LLaMA 기반 무료 필터로,
기존 임베딩 테이블과 비교해 빠르게 스캠 여부를 판단한다.
비용 없이 대량 처리가 가능하다.

2 단계는 GPT 기반 정밀 분석으로,
새로운 유형의 스캠이거나 애매한 경우에만 호출된다.
GPT 가 분석한 결과는 마스킹 후 DB 에 저장되고,
다음부터는 LLaMA 가 처리할 수 있게 된다.

즉,
새로운 스캠 → GPT 분석 → 의미 벡터 저장 → 이후 LLaMA 가 처리
이 흐름이 반복되면서 필터가 점점 더 똑똑해지는 구조다.

Q4. 왜 스캠을 자동 차단하지 않고 알림만 띄우나요?

정확도가 100%가 아닌 이상,
문자를 자동으로 차단하거나 삭제하면 **정상 메시지를 잃어버릴 위험**이 있다.
특히 고령층은 중요한 문자(병원, 은행, 가족 연락)를 놓치면 더 큰 문제가 생길 수 있다.

그래서 ScamX 는

- 스캠 의심 시 알림만 제공하고
- 사용자가 직접 판단할 수 있도록 하고
- 알림을 누르면 상세 분석 결과와 대처 방법을 보여주는 방식으로 설계했다.

정책적으로도 이 방식이 가장 안전하고 합법적이다.

Q5. 고령층이 알림을 놓치면 어떻게 하나요?

ScamX 는 고령층 사용성을 고려해 다음과 같은 UX 를 적용했다.

- 알림이 상단바에 일정 시간 유지
- 알림 센터에서 다시 확인 가능
- 클릭 시 상세 분석 페이지로 이동

추가로,
알림 지속 시간을 조절할 수 있는 옵션도 제공할 예정이다.
고령층이 놓치지 않도록 여러 단계에서 확인할 수 있는 구조다.