2025년 AI 라이프 아이디어 챌린지 제안서

<table>
<tr><td>아이디어명</td><td>디지털 취약 계층의 사기 피해 방지를 위한
실시간 다중 분석 AI 에이전트 기반 모바일 방어 시스템</td></tr>
<tr><td>제안자</td><td></td></tr>
<tr><td>제안서요약
(5줄 이내)</td><td>ㅇ 고령층 대상 신종 디지털 및 AI 사기가 급증하나 기존 방어 체계는 한계가 명확
ㅇ 백그라운드에서 실행되는 AI가 스마트폰의 모든 활동을 실시간 분석 및 위험 구역에 사전 방문하여 사기 위험을 복합적으로 방어하는 시스템
ㅇ On-Device AI, Cloud Sandbox, RAG 모델을 활용한 실시간 다중 분석 기술이 서비스 구현의 핵심 요소
ㅇ 기술적 방어를 넘어 인적 안전망을 결합한 하이브리드 케어 서비스임
ㅇ 사기 피해 예방, 정보 격차 해결, 가족의 심리적 안정 등 높은 사회적 가치를 창출</td></tr>
<tr><td>제안배경</td><td>ㅇ 디지털 안전의 사각지대, 심화되는 정보 격차
- 고령층 등 디지털 취약 계층의 스마트폰 보급률 및 금융 앱 사용률 급증
- 반면 디지털 정보 이해 및 위협 대응 능력은 현저히 부족
- 사회적 고립감, 건강 염려, 자녀 걱정 등 심리적 취약점을 악용한 범죄의 핵심 표적으로 부상
- 피해 발생 시에도 상황을 인지하지 못하거나 자책감으로 인해 신고를 꺼려 실제 피해 규모는 통계 이상으로 추정
ㅇ 날로 지능화·고도화되는 디지털 금융 사기 위협
- 전통적 사기: 택배 조회, 건강검진 안내, 자녀 사칭 등 사회공학적 기법 활용한 전통적 스미싱/피싱 수법이 여전히 높은 빈도로 발생
- 신유형 사기 AI 기술을 악용한 신종 범죄의 출현으로 위협 수준 급상승 (딥페이크 영상통화 자녀 사칭, AI 음성합성을 통한 가족 및 지인 목소리 보이스피싱 등)
ㅇ 기존 방어 체계의 명백한 한계
<table>
<tr><th>구분</th><th>기존 방어 시스템 (백신/차단 앱)</th><th>제안 시스템 (AI 에이전트)</th></tr>
<tr><td>핵심 타겟</td><td>일반 사용자</td><td>디지털 취약 계층 (고령층 등)</td></tr>
<tr><td>방어 방식</td><td>DB 기반 (알려진 위험, 블랙리스트)</td><td>AI 기반 (맥락, 이상행위, 패턴 분석)</td></tr>
<tr><td>방어 초점</td><td>기술적 공격 (바이러스, 악성코드)</td><td>사회공학적 공격 및 심리적 취약점</td></tr>
<tr><td>방어 범위</td><td>알려진 바이러스, 스팸 문자/전화</td><td>신종/변종 사기, 기만적 광고, AI 피싱</td></tr>
<tr><td>핵심 한계</td><td>사용자의 직접적인 판단/개입 요구</td><td>시스템의 선제적 분석 및 자동 개입</td></tr>
<tr><td>차별점</td><td>개별적·독립적 방어</td><td>보호자 연계를 통한 이중 안전망 구축</td></tr>
</table></td></tr>
</table>

	ㅇ **상황의 심각성과 새로운 방어 패러다임의 필요성** - 디지털 사기 범죄는 단순한 금전적 피해를 넘어 한 개인과 가정 전체에 깊은 정신적 고통과 무력감을 유발하는 심각한 사회 문제 - 단편적·사후적 대응에서 벗어나, 사용자가 인지하기 전에 시스템이 먼저 위협의 '맥락'을 분석하고 개입하는 선제적 방어 개념으로의 전환이 시급 - 기술적 방어와 인적 안전망을 결합하여 디지털 취약 계층을 실질적으로 보호할 수 있는 새로운 차원의 통합 방어 시스템 구축이 절실히 요구
아이디어 (제안내용)	ㅇ **아이디어 개요: 24시간 부모님과 동행하는 AI 디지털 경호원** - **솔루션 형태:** 자녀가 부모님 스마트폰에 한 번만 설치해드리면 이후 어떠한 조작도 없이 백그라운드에서 24시간 자동으로 작동하는 모바일 애플리케이션 **'AI 안심 가드(가칭)'** - **기술 구조** ▪ **On-Device AI:** 개인정보 보호를 위해 메시지, 화면 등 민감 정보는 외부 서버 전송 없이 스마트폰 내부에서 1차 분석 ▪ **Cloud Sandbox:** 의심스러운 URL은 격리된 클라우드 가상 환경에서 AI가 먼저 방문하여 안전성을 검증 ▪ **RAG (검색 증강 생성) 모델:** 최신 사기 사례 DB(경찰청, KISA)를 실시간으로 참조하여 알려지지 않은 신종 패턴까지 탐지 - **핵심 작동 방식:** AI 에이전트가 문자, 메신저, 웹서핑 등 모든 디지털 활동을 실시간으로 감시하며, 위협의 '맥락'을 다중 분석 - **주요 기능** ▪ **선제적 위험 탐지 및 차단:** 피싱, 스미싱, 악성 앱 설치, 기만적 광고 등 위험 감지 시, 사용자의 행동을 즉시 중단시키는 직관적 경고(전체 화면+음성) 발생 ▪ **보호자 연계 알림:** 위험 발생 및 차단 즉시, 사전에 등록된 자녀(보호자)에게 상황을 구체적으로 알려주는 안심 알림 발송 ▪ **지속적 학습 및 업데이트:** 경찰청, KISA 등의 최신 사기 사례 DB를 AI가 지속적으로 학습하여 신종 범죄 패턴에 자동 대응 ㅇ **서비스 목적: 기술로 구현하는 디지털 안심과 가족 연결** - 궁극적 목표: 디지털 취약 계층의 금융 자산 및 개인정보를 모든 종류의 디지털 사기로부터 선제적으로 보호하고, 가족 구성원 모두의 심리적 안정감 확보 - 정량적 목표 ▪ 악성 URL/피싱 사이트 클릭률 90% 이상 감소 ▪ 출처 불명 악성 앱(apk) 설치율 제로(Zero)화 ▪ 위험 상황 발생 시 5초 이내 보호자 알림 도달률 99% 달성 - 정성적 목표 ▪ 어르신 세대의 스마트폰 사용 불안감 해소 및 디지털 정보 격차 완화 ▪ 자녀 세대의 부모님 걱정 경감 및 '디지털 효도' 만족감 제공 ㅇ **다층 방어 체계를 통한 빈틈없는 위협 대응** - **1차 방어망: AI 기반 실시간 탐지** ▪ 수신되는 문자/메신저, 접속 웹페이지 등을 AI 에이전트가 실시간으로

분석
  - '자녀 사칭', '기관 사칭', '악성 URL 패턴' 등 사회공학적 맥락과 이상 행위를 즉시 탐지
- **2차 방어망: 직관적 경고 및 즉시 차단**
  - 사용자가 위험 링크를 클릭하거나 악성 앱 설치를 시도하는 등 위험 행동 시 즉시 개입
  - 화면 전체를 덮는 경고창과 음성 안내를 통해 사용자가 명확히 위협을 인지하고 행동을 중단하도록 유도
- **3차 방어망: 보호자 연계를 통한 이중 안전망**
  - 위협 탐지 및 차단 즉시, 사전에 등록된 보호자(자녀 등)에게 구체적인 상황 알림 발송
  - 기술적 방어가 실패하는 최악의 경우에도 보호자의 신속한 인적 개입을 유도하여 2차 피해 방지

예상되는 기술구현 (AI) 과정에서 유의점

ㅇ 기술 구현 문제점 및 해결방안

구분	예상 문제점 (Potential Issues)	해결 방안 (Solutions)
성능 및 안정성	24시간 백그라운드 작동으로 인한 배터리 과다 소모 및 스마트폰 성능 저하 우려	- On-Device AI 중심 설계: 서버 통신 최소화 및 기기 연산 활용 - 경량 AI 모델 적용: 모바일 최적화 모델로 리소스 점유율 최소화
AI 탐지 정확도	오탐지(정상 메시지/광고를 위협으로 판단)로 인한 사용자 피로도 증가 및 신뢰도 하락	- 위험도 등급 시스템: '의심-경고-위험' 3단계 세분화 - 사용자 피드백 루프: '오탐지 신고' 기능으로 AI 학습 및 보정
개인정보 보호	민감한 개인정보 접근에 따른 심리적 저항감 및 데이터 유출 우려	- 데이터 처리 투명성 강화: 수집·분석 데이터 명확 고지 - 데이터 비식별화: 개인 식별 정보는 원천 수집·저장 차단
지속적인 위협 대응	신종 사기 수법 등장으로 기존 AI 모델의 탐지 능력 저하 가능성	- RAG 모델 활용: 최신 사기 사례 DB와 실시간 연동 학습 - 주기적인 모델 업데이트: 신규 위협 대응 로직 지속 추가

기대효과

ㅇ 정량적 효과
- 디지털 금융 사기 피해 가능성 50% 이상 감소: AI의 선제적 탐지 및 다층 방어 체계를 통해 잠재적 사기 시도를 원천적으로 차단
- 스미싱 URL 클릭 및 악성 앱 설치율 50% 이상 차단: 위험 행동을 즉시 중단시켜 악성코드 감염 및 정보 탈취 경로를 봉쇄
- 사기 피해 발생 시 보호자 인지를 통한 골든타임 확보 및 2차 피해 확산 방지

ㅇ 정성적 효과
- 사용자) 스마트폰 사용에 대한 막연한 불안감 해소 및 디지털 자신감 향상
- 보호자) 부모님의 디지털 안전에 대한 걱정 경감 및 심리적 안정감 확보
- 가족) '디지털 효도'라는 새로운 소통 문화를 통해 세대 간 유대감 강화

ㅇ 기술·산업적 효과
- On-Device AI와 RAG 모델을 보안 분야에 적용한 선도적 기술력 확보

	- 기존 보안 시장을 **'디지털 케어 서비스'**라는 새로운 시장 개척 및 선도 - 시니어 테크 시장 활성화 및 관련 AI 기술 생태계 구축에 기여 **ㅇ 사회·문화적 효과** - 디지털 사기 범죄로 인한 막대한 사회적 비용(수사, 복구 등) 절감 - 세대 간 디지털 정보 격차 해소에 기여하는 대표적인 '따뜻한 AI' 성공 사례 제시 - 기술을 통해 사회 문제를 해결하고, 더 촘촘한 사회 안전망을 구축하는 긍정적 선례 마련

【유의사항】

ㅇ 제안내용이 他 공모전 수상 및 타인의 저작물 모방 혹은 표절 등으로 확인될 경우 심사 대상에서 제외될 수 있으며, 결과발표 이후라도 수상 취소 및 상금환수 등의 조치를 취할 수 있습니다.
ㅇ 제안내용과 관련하여 초상권, 저작권, 명예훼손 등의 문제발생 시, 일체의 법적·도의적 책임은 제안자(응모자)에게 있습니다.
ㅇ 공모전 내용 및 심사규정의 제반조건에 동의하며, 이에 따른 결과와 관련하여 일체의 이의를 제기하지 않겠습니다.
ㅇ 심사위원의 심사결과에 따라 적합한 제안이 없다고 판단되는 경우, 수상작을 선정하지 않거나 수상대상 수를 임의 조정할 수 있음에 동의합니다.
ㅇ 제출된 서류는 일체 반환하지 않습니다.

【개인정보의 수집·이용에 관한 사항】

한국산업기술기획평가원은 AI 라이프 아이디어 챌린지의 운영·관리를 위하여 아래와 같이 귀하의 개인정보를 수집·이용하고 있으며, 이 정보는 동 목적으로 제3자에게 제공됩니다.

ㅇ 개인정보의 수집이용 목적 : 챌린지(공모전) 접수, 검토, 심사, 선정 결과 발표
ㅇ 수집·이용할 개인정보 항목 : 성명, 소속, 생년월일, 휴대전화번호, 이메일
ㅇ 개인정보를 제공받는 자 : 중복검토를 위한 타 공공기관 등
ㅇ 개인정보의 보유 및 이용기간 : 챌린지(공모전) 결과 발표 후 1년, 수상작의 경우 5년

※ 귀하는 상기 동의를 거부할 수 있습니다. 다만, 이에 대한 동의 하지 않을 경우, 운영 절차상 부득이하게 공모전 참가 신청이 거부됨을 알려드립니다.

위와 같이 개인정보를 수집·이용하는데 동의하십니까? ■ 동의함 □ 동의하지 않음

본인은 한국산업기술기획평가원이 주최하는 2025년 AI 라이프 아이디어 챌린지에 참가하며, 동 내용에 대한 공고내용을 충분히 숙지하였고, 제안하는 내용 관련하여 타(他) R&D 사업, 타(他) 공모전(챌린지) 등에 제출한 바가 없음을 확인합니다.

2025년 9월 30일 [redacted]

[redacted]

한국산업기술기획평가원장 귀하