



M-Security

시니어 맞춤 피싱 감지 웹

CONTENTS



프로젝트 김영이

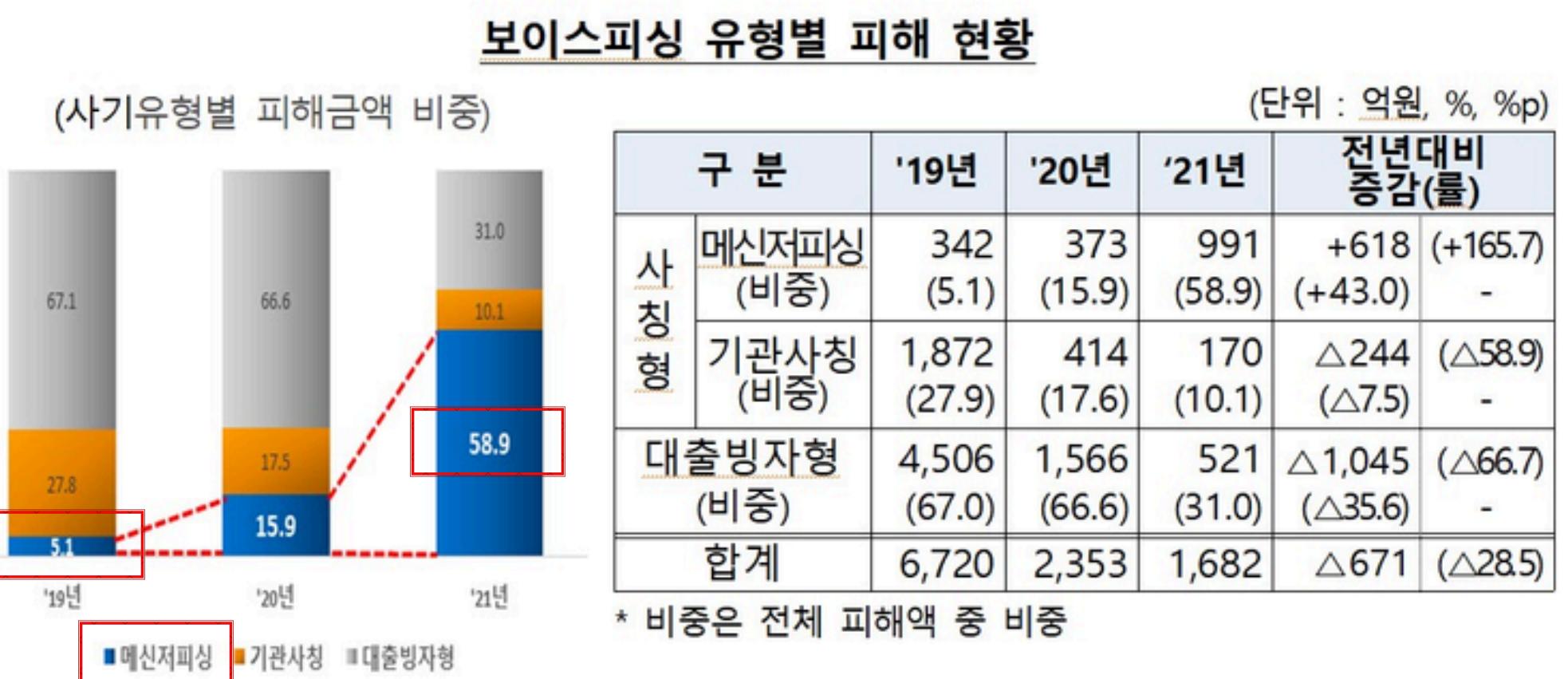
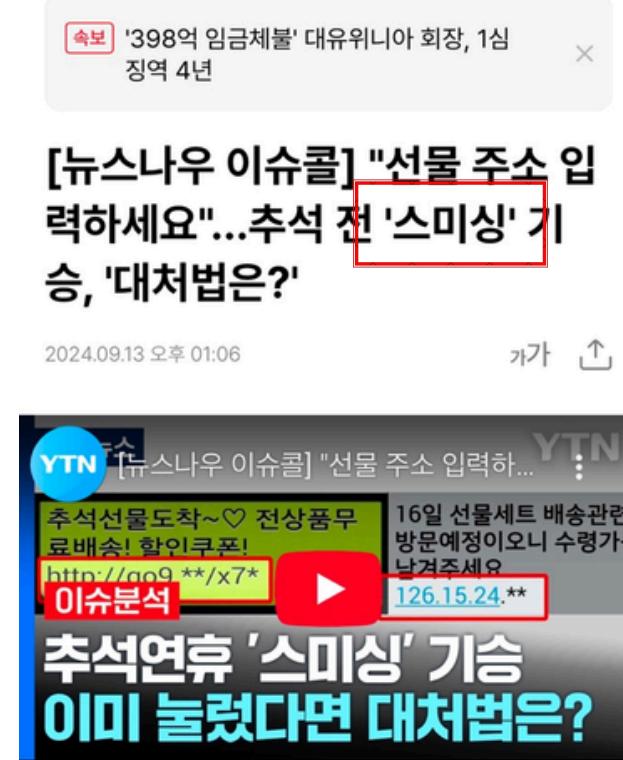
- 01 ━━━━━━━━━━━━━━━━ 기획의도 및 웹 소개
- 02 ━━━━━━━━━━━━━━━━ 시스템 아키텍처
- 03 ━━━━━━━━━━━━━━━━ 멘토링을 통해 수정/보완한 내용
- 04 ━━━━━━━━━━━━━━━━ 주요기능 및 사용방법
- 05 ━━━━━━━━━━━━━━━━ 기대효과 및 추진방향
- 06 ━━━━━━━━━━━━━━━━ 사용자 피드백
- 07 ━━━━━━━━━━━━━━━━ 구현링크 & 스크린샷
- 08 ━━━━━━━━━━━━━━━━ 참고문헌 및 출처

01

기획의도- 배경

"메신저 피싱과 시니어 대상 피싱 범죄율의 지속적인 증가"

YTN 사회
LIVE
홈 정치 경제 사회 연예 게임



* 피해구제신청접수(1차 계좌) 기준(법인 제외)

출처 : 2023년 보이스피싱 피해현황 분석

출처:

YTN 2024.09.13 기사, 금융감독원

프로젝트 배경

5개국어 글로벌 경제지

AI 자동번역 2025.02.19 (수) 中文 |

아주경제

중국 AI 산업 재테크 경제 정치 사

목호노인종합복지관, "보이스 피싱, 알아야 속지 않는다"

이동원 기자 | 입력 2023-07-05 09:40

◇ 지난해 60대 이상 보이스피싱 피해액 614억… 전체 37% 차지

위 사건은 실제 지난해 말 금융감독원에 접수된 지인 사칭 메신저피싱 사례다. 금융감독원에 따르면, 2021년 국내 보이스피싱 피해 금액은 총 1682억원으로, 코로나19에 따른 사기활동 감소와 함께 2020년보다 671억원 줄었다. 60대 이상 고령자의 피해금액 역시 2020년 686억원에서 2021년 614억원으로 70억원가량 감소했다. 그러나 피해 금액만 줄었을 뿐, 전체 피해연령 중 60대 이상이 차지하는 비중은 계속해서 늘고 있다. 2019년에는 약 26.5% 수준이었으나, 지난해는 37%로 2년 만에 10% 이상 증가했다. 같은 기간 20·30대와 40대 피해 비중이 줄어든 것과 대비된다. 국내 고령 인구가 계속해서 증가하고 있는 가운데, 젊은 층에 비해 보이스피싱 범죄에 대한 경각심이 낮고 정보가 부족한 노인들의 피해가 늘어난 것으로 풀이된다.

시니어가 피싱에 취약한 이유

디지털 환경에 대한 낮은 이해도

정보 공유 부족 / 교육기회 제한

공식 기관에 대한 높은 신뢰

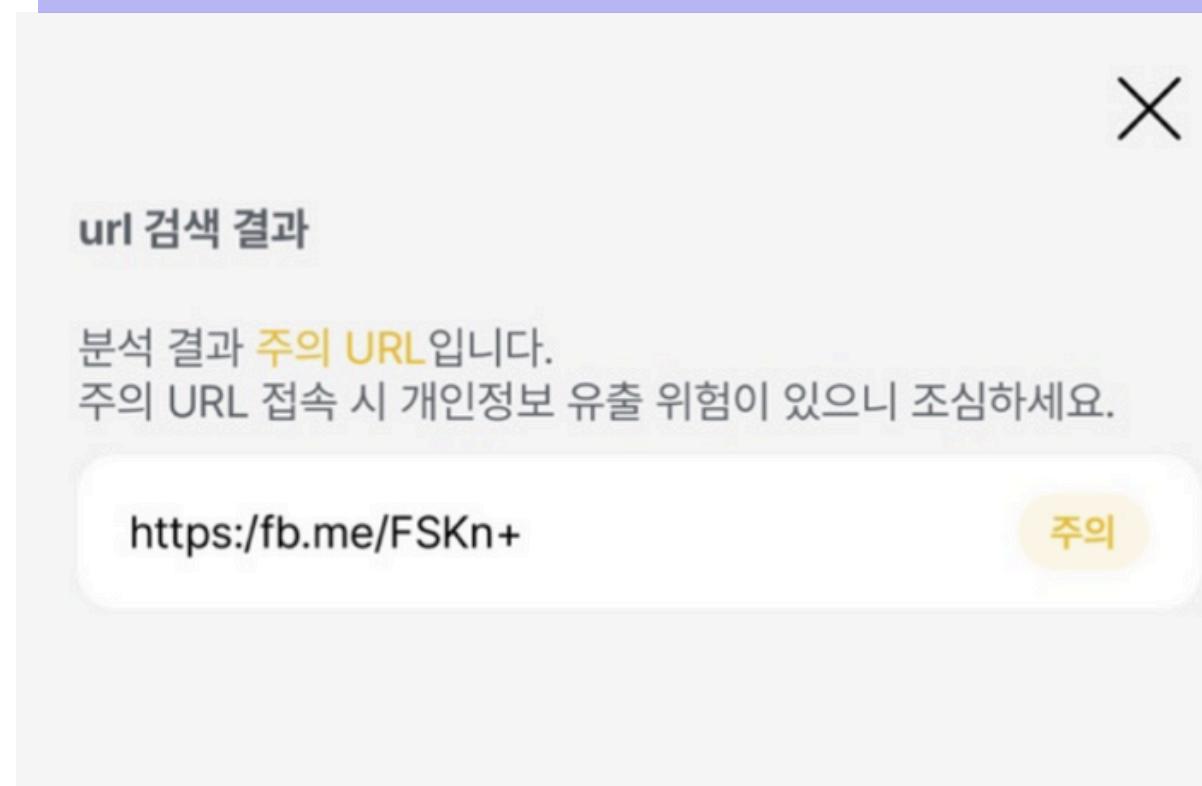
→ 시니어들이 쉽고 편리하게 활용할 수 있는 사용자 친화적 웹·앱의 필요성

출처:

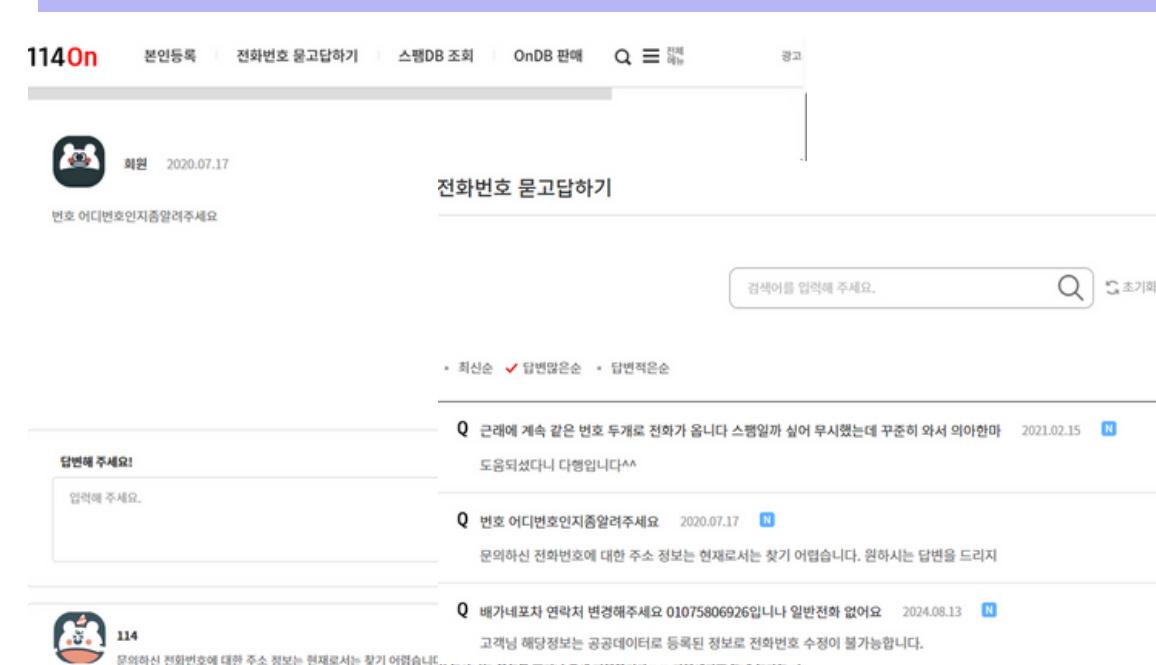
2023.07.05 아주경제 기사, 2022.06.03 헬스조선 기사

기획의도 - 참신성/독창성

후후 피싱 여부만 알려주는 한계점



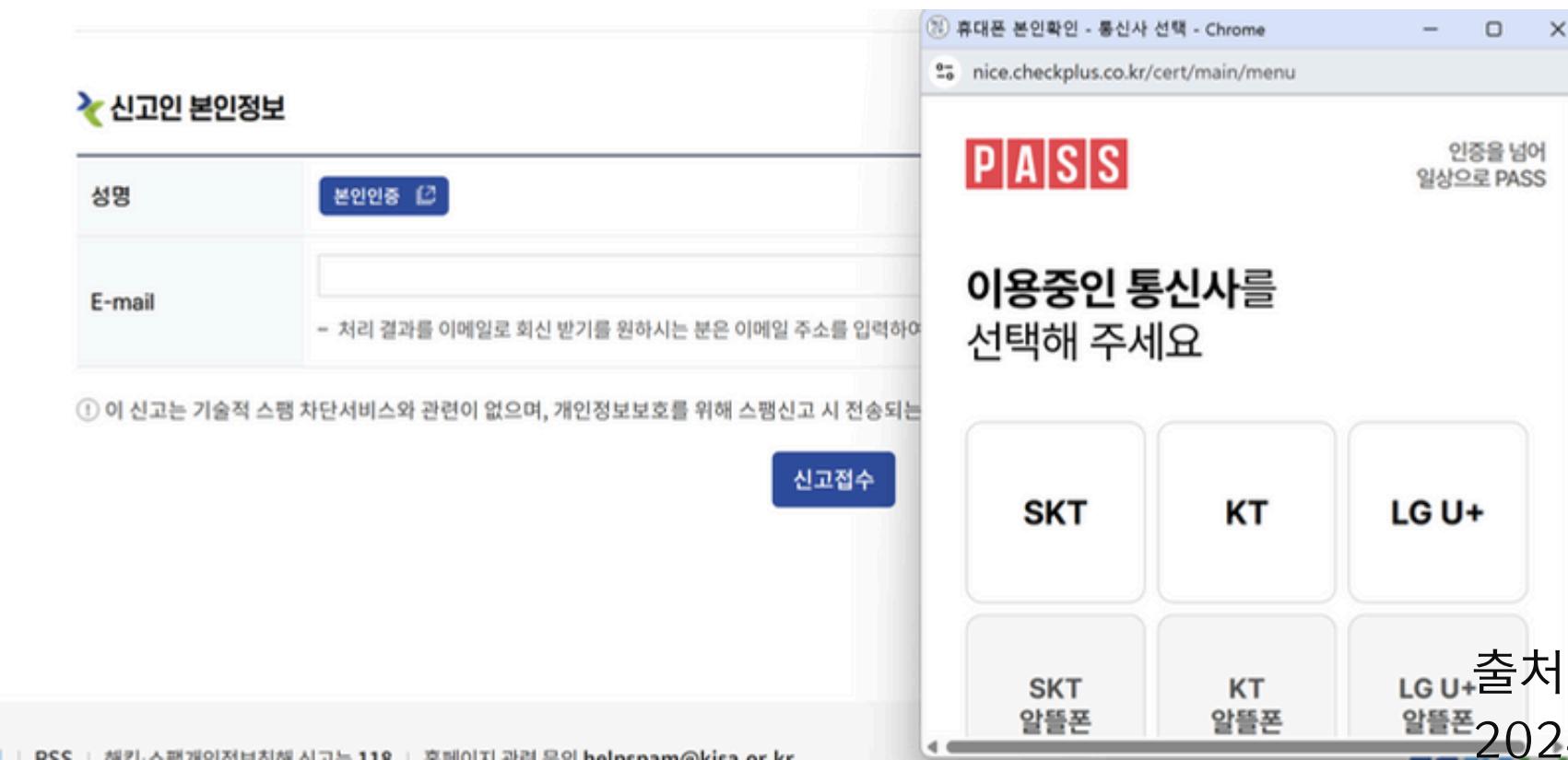
114on 부족한 커뮤니티 기능



KISA 서비스 시니어에게 어렵고 번거로운 검사 및 신고 절차

하지만 6개월이 지난 지금도 갈 길이 먼 모습이다. 우선 사용자 편의성이 떨어진다는 지적이 나온다. 스미싱 메뉴를 누르지 않고 바로 보호나라 채널 채팅창에 URL을 넣으면 제대로 된 답을 내지 못한다. 실제 포털 사이트 네이버라는 설명과 함께 네이버의 URL을 채팅창에 바로 입력한 결과 답변이 어렵다는 채팅이 돌아왔다.

별도로 스미싱 버튼을 눌러 입력한 결과도 마찬가지다. "확인되지 않은 링크"라며 우선 주의 메시지부터 보낸다. 당초 KISA는 안전성이 검증된 URL 화이트리스트를 축적해 판독 속도를 높이겠다고 밝힌 바 있다. 하지만 KISA의 설명과 달리 판독에는 오랜 시간이 걸렸다. 네이버뿐만 아니라 서비스를 제공하는 KISA 공식 홈페이지 또한 주의해야 할 URL로 안내했다.





피싱지킴이 창의적 요소

"이런 툴이 있었으면 좋겠다고 생각했습니다."



화이트리스트/블랙리스트 기반 피싱 탐지

신뢰기관 DB + 사기의심 DB 를 크롤링하여 검증된 기관인지 확인

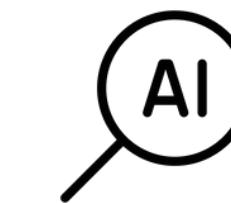


기하급수적으로 증가하는 사기번호와 URL

왜 피싱인지 알 수 없다는 한계

무지나 실수로 인한 피해 가능성이 큰
시니어를 위한 서비스의 부재

어렵고 번거로운 신고절차



AI 기반 피싱 분석

단순 검출이 아닌 왜 피싱인지/피싱이 아닌지 AI를 통한 설명



시니어 친화적인 UI/UX

글씨 크기 조절 및 음성 기능 추가, 간단한 작동 방식



커뮤니티 투표

사용자들이 직접 의심 사례를 평가하고 공유하며 집단지성 활용

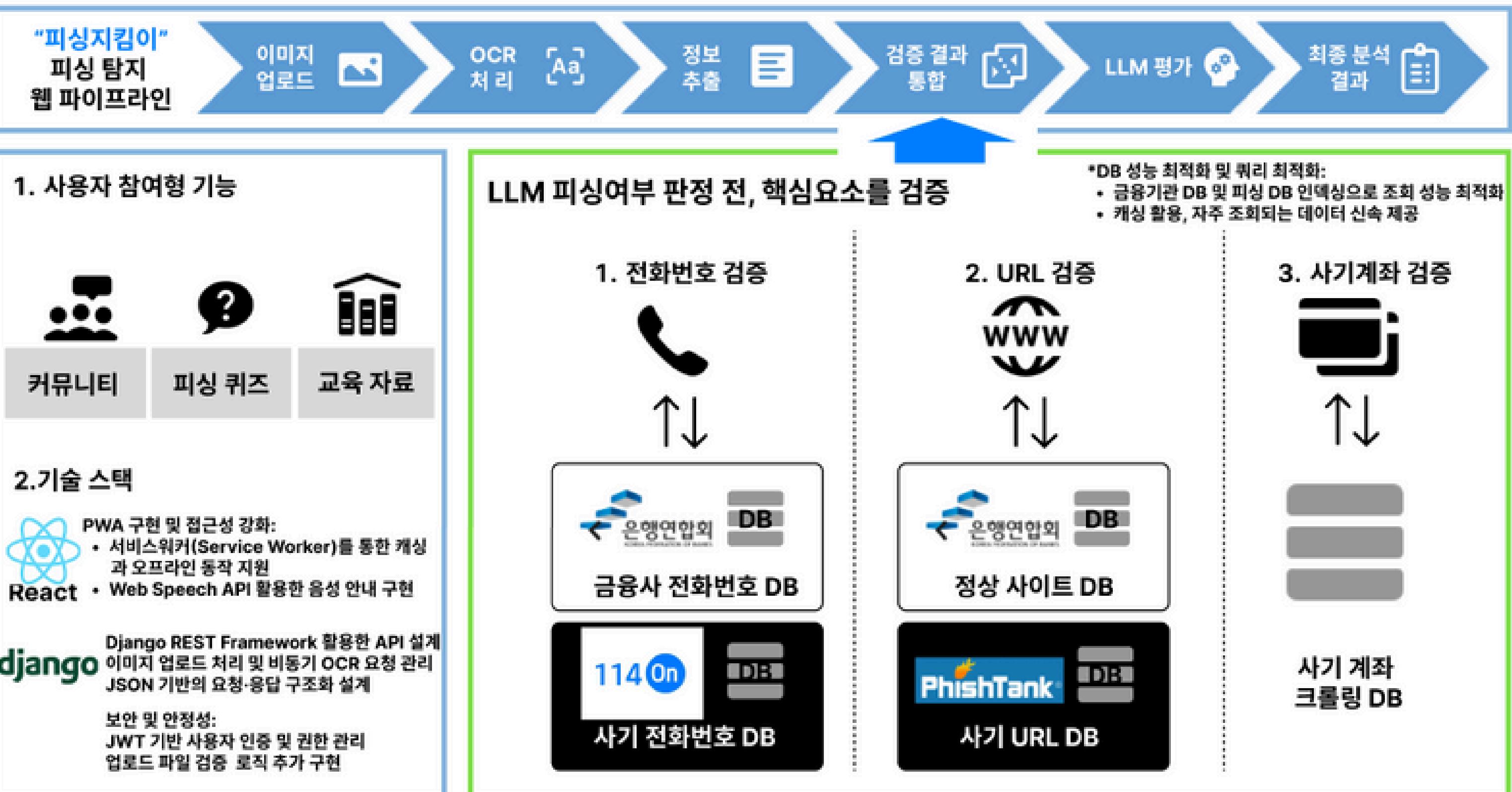


원스톱 신고

이미지 속 URL, 전화번호, 계좌번호 검사와 신고까지 한 번에 처리

02

시스템 아키텍처



멘토링을 통해 수정/보완한 내용

① UI 단순화

검사 시작하기

개별 항목 검사하기

URL 검사
검사할 URL을 입력하세요

전화번호 검사
전화번호를 입력하세요

계좌번호 검사
계좌번호를 입력하세요

개별 항목 검사 - URL



이미지로 한번에 검사하기

클릭하여 이미지 업로드하기

안심하세요
업로드한 이미지는 분석에만 사용되며 저장되지 않습니다.

입력해서 검사하기

모바일/데스크톱에서 편하게 이용하실 수 있도록 앱 설치를 권장드립니다.

② 교육자료 수정

영상 자료
스미싱 관련 교육 및 예방 영상

스미싱 특징
① 스미싱 특징 영상 1
② 스미싱 특징 영상 2

예방 및 대응
① 예방 및 대응 영상 1
② 예방 및 대응 영상 2

스마트폰 보안 설정
기기별 스미싱 예방 설정 방법

갤럭시 원UI 6.0 설정

1단계
설정 → 보안 및 개인정보 보호 → 보안 위험 차단 → 사용 중 활성화해 주세요

2단계
각 항목 활성화해 주세요
• 메시지 앱 보호: 메시지로 오는 다운로드 차단 해 주세요
• USB 케이블을 사용한 소프트웨어 업데이트 차단: 유선 헤킹으로부터 보호해 주세요

갤럭시 원UI 5.0 이하 설정



영상 자료
스미싱 관련 교육 및 예방 영상

스마트폰 보안 설정
기기별 스미싱 예방 설정 방법

스미싱 특징
스미싱 특징 영상 1

엄마 번호로 전화 있는데 보이스피싱이었다(?)

스미싱 특징 영상 2

"결혼식에 많이 와주세요!"
모바일 청첩장 놀렸더니 4천만원 증발?

원 UI 6.0 업데이트를 지원하는 최신 갤럭시 스마트폰
해당 기능을 켜면 외부앱 설치가 차단됩니다.

③ 개인정보처리방침 고지 추가

주의사항
사진 내에 개인정보가 포함되지 않게 주의해 주세요! (또는 최대한 가려 주세요)
주민등록번호, 계좌번호, 연락처, 주소 등의 개인정보는 피싱 공격에 악용될 수 있습니다.

회원가입

아이디를 입력해주세요

이메일을 입력해주세요

비밀번호를 입력해주세요

× 8자 이상어야 합니다.
× 대문자를 포함해야 합니다.
× 특수문자를 포함해주세요
× 숫자를 포함해주세요

비밀번호를 다시 입력해주세요

개인정보 처리방침에 동의합니다. [전문보기](#)

회원가입

개인정보 처리방침

- 수집하는 개인정보 항목
 - 필수항목: 아이디, 이메일 주소, 비밀번호
 - 개인정보의 수집 및 이용목적
 - 서비스 제공을 위한 회원 식별 및 본인 확인
 - 서비스 이용에 따른 본인확인, 개인 식별
 - 불량회원의 부정 이용 방지와 비인가 사용 방지
 - 고지사항 전달, 불만처리 등을 위한 원활한 의사 소통 경로의 확보
 - 개인정보의 보유 및 이용기간
 - 회원 탈퇴 시까지
 - 단, 관계 법령에 의해 보존할 필요가 있는 경우 해당 법령에 정한 기간 동안 보존
- 개인정보의 파기절차 및 방법
 - 회원 탈퇴 시 즉시 파기
 - 전자적 파일 형태로 저장된 개인정보는 기술적 방법을 사용하여 완전히 삭제
- 개인정보의 안전성 확보 조치
 - 개인정보의 암호화
 - 해킹이나 컴퓨터 바이러스로부터 보호하기 위한 보안프로그램 설치
 - 개인정보에 대한 접근 제한

이미 계정이 있으신가요? [로그인](#)

④ 원터치 신고 기능 추가

이미지에서 발견된 정보

계좌번호

434-2252

신고하기

신고 접수 완료!

X

신고해주시셔서 감사합니다. 검토 후 데이터베이스에 등록 됩니다.

확인

+ 기술적 추진방향 및 목표수립 보완

주요 기능 및 특징

이미지 기반 피싱 자동 탐지

- 이미지 업로드 한 번으로 전화번호·계좌·URL 등
시 탐지
- LLM(대형언어모델) 기반 텍스트 피싱 여부 분석
- 최신 논문 적용 피싱판별 기준 활용

금융기관 DB 기반 신뢰도 검증

- 7000여 개 금융기관·카드사·보험사 공식 전화번호
DB 구축
- 등록 번호 여부 및 기관명 즉각 확인 가능
- 화이트리스트·블랙리스트 교차검증 시스템 제공

시니어 특화 사용자 경험(UX)

- 직관적인 대형 폰트와 고대비 인터페이스 제공
- 피싱 탐지 결과 음성 안내 지원
- 네이티브 앱 같은 사용성의 PWA 기반 서비스

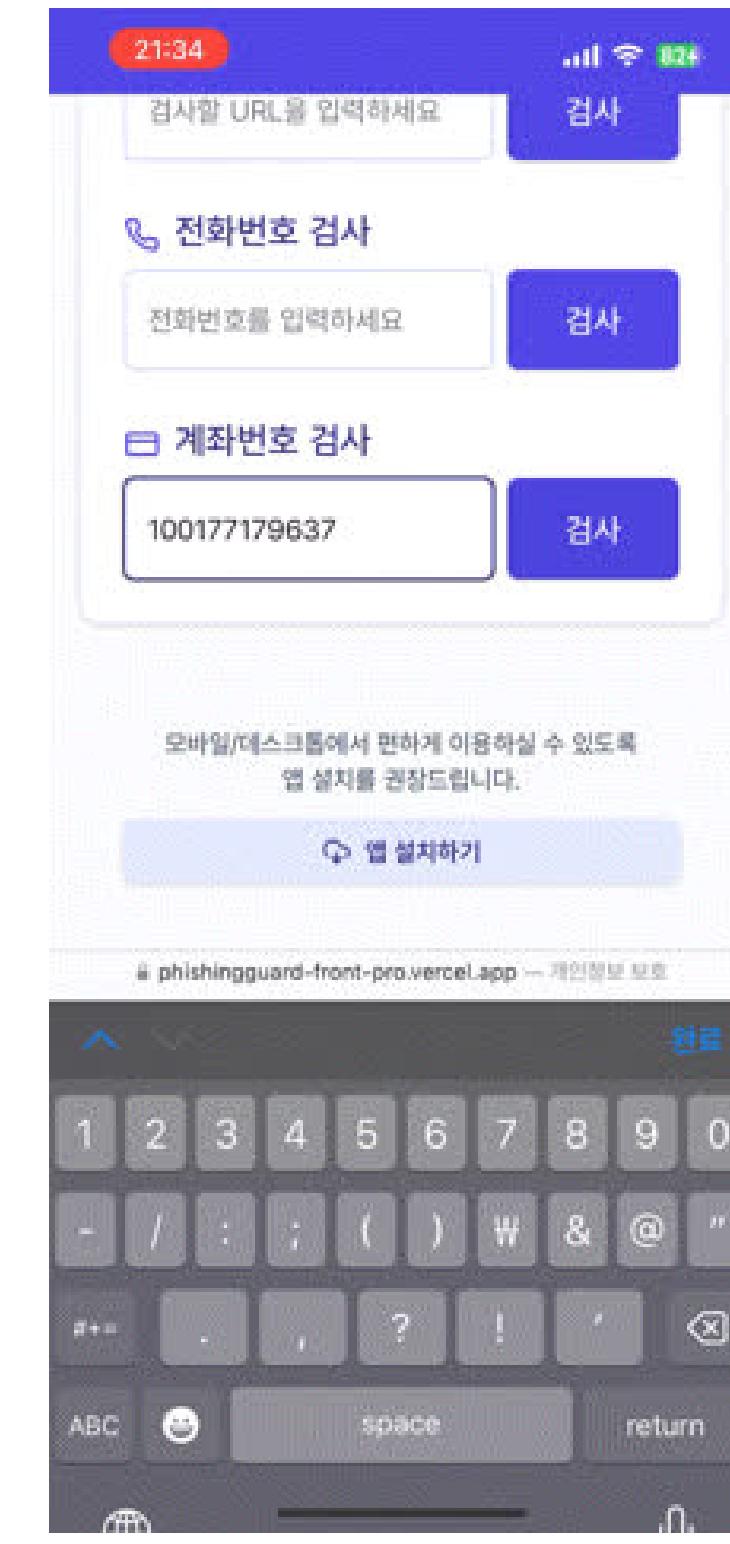
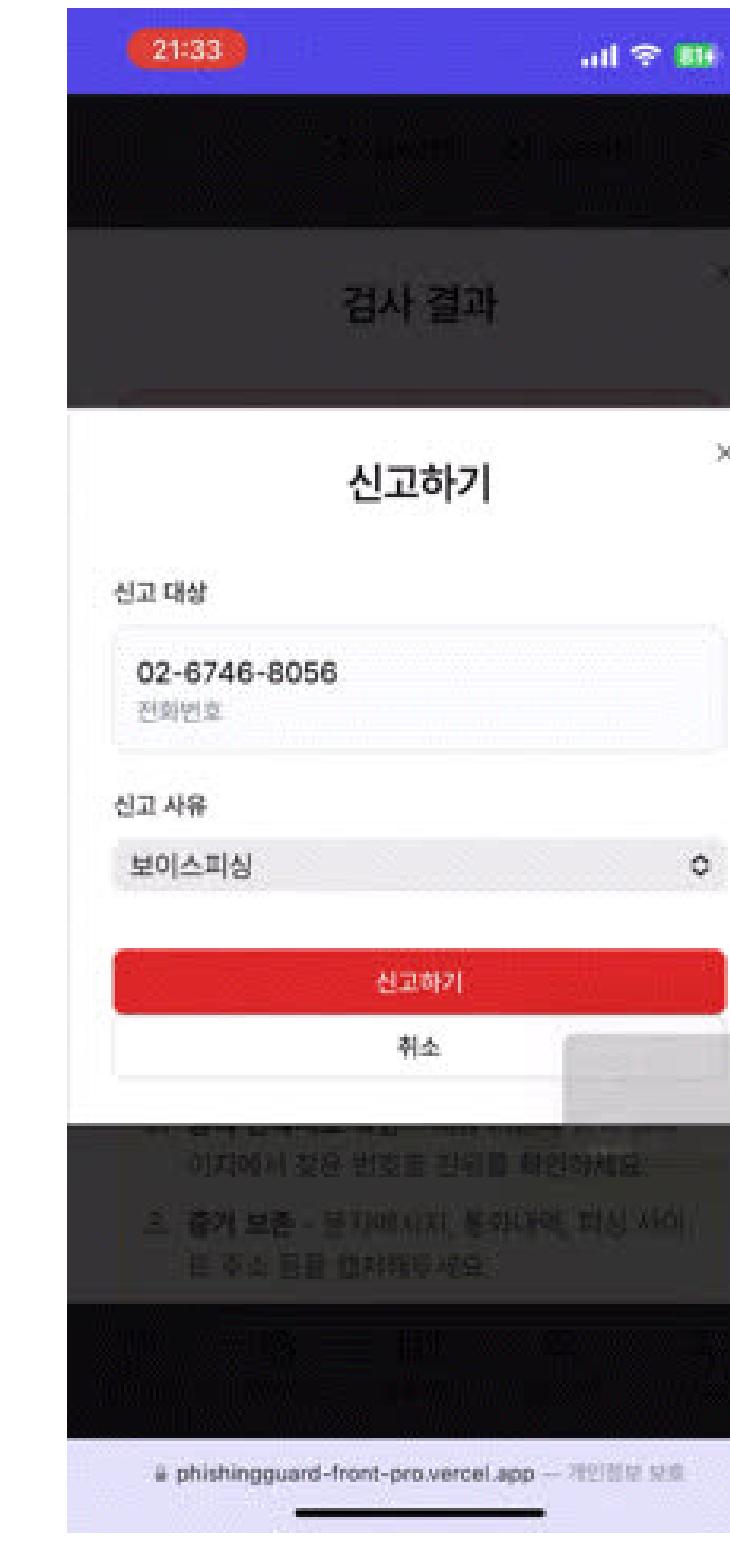
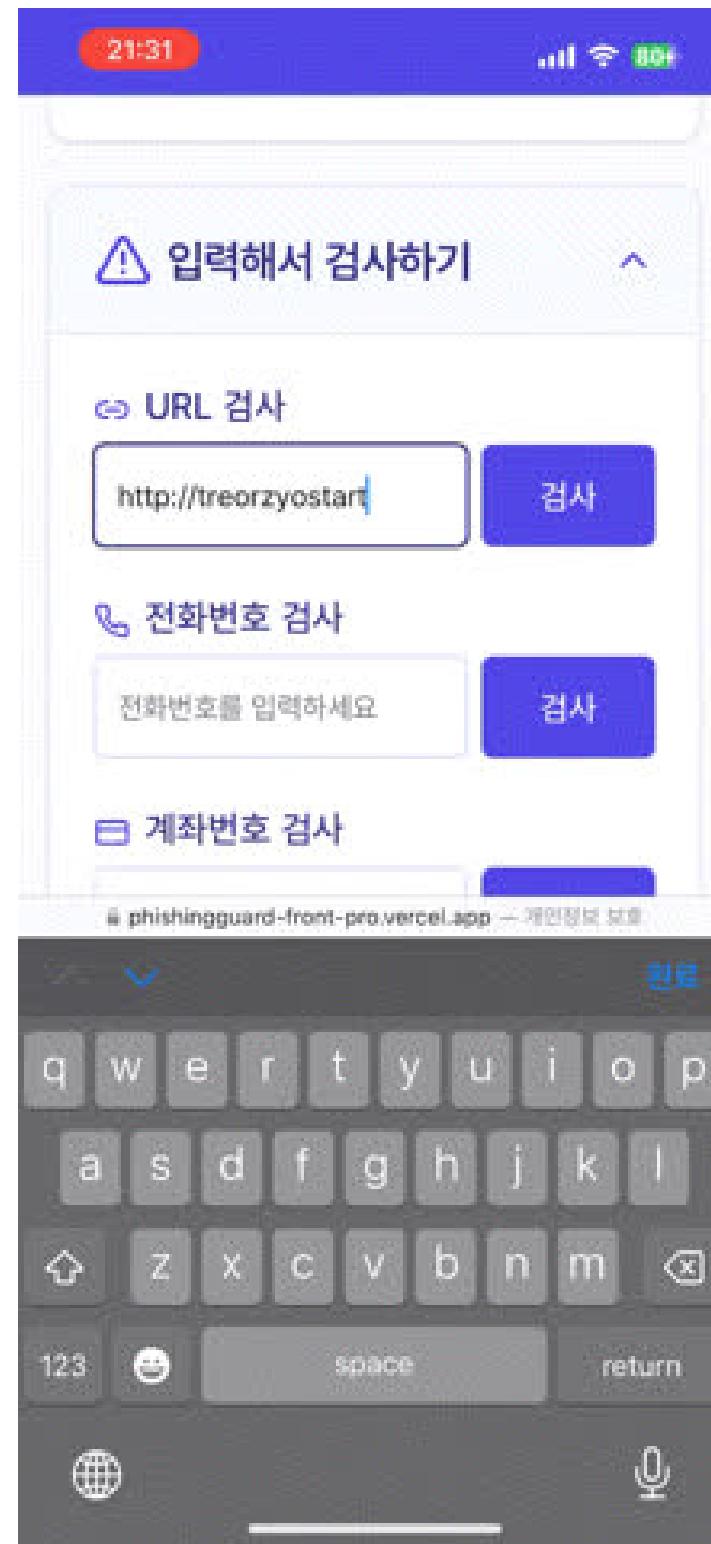
집단지성·게임피케이션 기반 보안 교육

- 커뮤니티 기반 피싱 사례 공유 및 투표
- 퀴즈·랭킹·뱃지 기능을 통한 흥미로운 교육
- 보안 뉴스 실시간 제공 및 AI기반 3줄 요약 지원

04

주요 기능
및
사용방법
(각 기능 영상 첨부)

-1) 개별검사





피싱검사 및 분석

신화면오 검사 결과
신고된 번호입니다: (총 843건 - 후후: 833건)
전화번호: 02-434-2252

이미지에서 발견된 정보
계좌번호: 434-2252

이미지 콘텐츠 분석
확인된 공식 전화번호가 없으므로 피싱 가능성을 판단해야 합니다. 메시지 내용은 뭇데카드 발급 완료를 알리는 것처럼 보이지만, 본인 요청이 아닐 시 즉시 문의하라는 긴급성을 강조하고 있으며, 저하번호 표기 방식이 다르게 나타나고 ('+82 2-434-2252' 와 '+82 2 434 2252'가 다른 번호로 처리되는 경우)

전화번호 검사

피싱검사
피싱과 사기를 검사합니다.

학습퀴즈
제미있게 배우는 피싱예방

교육자료
쉽게 이해하는 피싱예방

커뮤니티
함께 공유하는 정보

내정보
나의 활동 정보

선착순 마감이니 서둘러주세요!
무료수신거부: 080-877-5620

문자 메시지 · SMS

검사 시작하기

입력해서 검사하기

[피싱 문자 검사]

- ① 정규식+ OCR 기술을 활용한 사진 속 계좌번호, 전화번호, URL 자동 추출
- ② 추출된 정보는 자동으로 시스템에 입력되어, 신뢰기관의 [화이트리스트](#) DB 내의 인증된 금융기관인지 우선 확인하고, 없을 경우 사기 DB를 거쳐서 사기신고이력 조회
- ③ 두 DB 모두 정보가 없다면, 신고되지 않은 번호/URL이라고 표시
문자 등 분석할만한 내용이 있는 경우 AI 분석을 통한 피싱 상세분석 제공
대응방법과 관련 기관 신고절차에 대한 상세 가이드 제공 및 원터치 신고

[정상 문자 검사]

피싱 및 사기 검사

이미지로 한번에 검사하기
클릭하여 이미지 업로드하기

사진 확인하기
업로드한 이미지는 신뢰한 사용자가 저장되었습니다.

입력해서 검사하기

피싱검사 학습퀴즈 교육자료 커뮤니티 내정보

ngguard-front-pro.vercel.app

[모바일 버전]



피싱교육

피싱 퀴즈

Level 5 80/100

퀴즈 랭킹

| 순위 | 유저명 | 점수 |
|----|------------|------|
| 1 | csy | 480점 |
| 2 | seoyun0807 | 480점 |
| 3 | flower | 430점 |
| 4 | bluesea | 390점 |
| 5 | sy0301 | 340점 |
| 6 | mangoo | 300점 |

[학습 퀴즈]

예방 및 대응 피싱 종류 및 대응법 신고 및 피해대응

영상 자료 스미싱 관련 교육 및 예방 영상

스마트폰 보안 설정 기기별 스미싱 예방 설정 방법

스미싱 특징 스미싱 특징 영상 1
스미싱 특징 영상 2

[교육 자료]

- ① “시니어”들을 위한 피싱 **교육형** 퀴즈 제공
- ② 퀴즈, 진행 현황, 랭킹, 뱃지 시스템이 결합된 게임형 피싱 학습 경험 제공
- ③ 신뢰할 수 있는 출처의 영상과 자료로 구성된 **교육자료** 제공

Q. 피싱 목적

피싱 공격의 주요 목적은 무엇인가?

- 사용자의 개인 정보를 탈취한다.
- 컴퓨터를 고장낸다.
- 인터넷 속도를 느리게 한다.
- 소프트웨어를 무료로 배포한다.

정답 제출하기

피싱검사 학습퀴즈 교육자료 커뮤니티 내정보

phishingguard-front-pro.vercel.app — 개인정보 보호

[모바일 버전]
• 소리기능



커뮤니티

Bandisoft.com 접속하기 빠르게 액세스하려면 즐겨찾기를 즐겨찾기 모음에 넣으세요. [지금 즐겨찾기 관리](#)

19:47 글씨크게 소리켜짐 S

피싱지킴이

게시물 상세

카드 발급.. 약 23시간 전

작성자: sy0301

저 롯데카드 만든 적이 없는데 이런 문자가 왔어요
전화해봐야 할까요?

문자 메시지 · SMS
1월 14일 (화) 오후 3:40

[Web발신]
[롯데카드]
/****27021 카드 저사바그아로

① 커뮤니티 댓글 및 투표(피싱같아요/피싱 아니에요) 기능으로 피싱 정보를 실시간 공유하고 상세 의견을 나눌 수 있으며, 신고된 번호도 조회 가능

② 커뮤니티 속 최신보안기사 요약 코너(업로드 자동화)를 통한 정보제공



[모바일 버전]

차별성

A사 앱서비스 / B사 앱서비스 / 피싱지킴이

| | 피싱검사 | 퀴즈/교육 | 사용자 커뮤니티 | 신고 | 접근성 |
|---------|------|-------|----------|----|-----------------------|
| A사 앱서비스 | O | X | X | X | 안드로이드 |
| B사 앱서비스 | O | △ | X | O | 웹(일부) 안드로이드 IOS |
| 피싱지킴이 | O | O | O | O | 웹 안드로이드 IOS |

05

기대효과

EXPECTATION 01.

- 이미지를 업로드하는 단순한 작업으로 피싱 탐지 및 예방 가능
- 대규모 DB 및 LLM을 활용해 더욱 신뢰도 높은 분석 결과 제공

EXPECTATION 02.

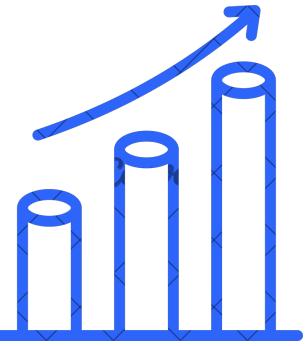
- 퀴즈와 교육자료를 통한 피싱 탐지 능력 향상 및 보안 인식 향상

EXPECTATION 03.

- 다양한 피싱 사례와 대응 방안을 공유하며 실질적인 통찰력 확보
- 보안 뉴스 업데이트로 최신 피싱 이슈 학습 가능

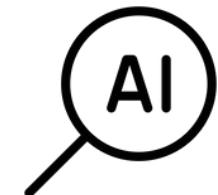
EXPECTATION 04.

- 시니어를 위한 직관적인 UI/UX로 접근성 강화
- PWA 기능을 적용하여 앱 설치 없이 가볍고 빠르게 실행 가능



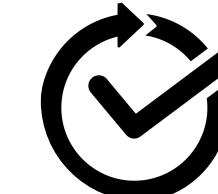
피싱지킴이 확장성

피싱 탐지 모듈 추가



- 이메일 캡쳐 및 내용분석을 통한 피싱여부 판단
- DNS 조회를 통한 도메인 생성일 조회
- 보이스분석 기반 피싱여부 판단

플러그인화



- 이미지에 플러그인을 연동하여 [공유] 버튼 클릭 시, 자동으로 [피싱지킴이]에 연동되며 원스톱 검사/신고 기능 제공
- 빅스비/시리 등 인공지능 비서 연동 가능



데이터 활용

- 사용자의 동의 후, 커뮤니티 내 자료 및 분석 업로드 자료를 활용하여 피싱 데이터셋 구축
- 개인정보 비식별화 후 피싱탐지 강화학습 등, 데이터 활용
- 자료 공유 및 판매



게이미피케이션

- 포인트 제도를 통한 상점 운영
- 프로필 꾸미기 뿐만 아니라, [물고기 키우기] 등 잣은 접속을 필요로 하는 게임 접목
- 랭킹 및 점수 발표를 통한 참여도 향상

추진방향 – 피싱지킴이 3단계 로드맵

① 초기 시장 진입 및 기반 구축

제품 안정화

- 기존 PWA 서비스의 버그 수정 및 성능 최적화
- 정기적 피싱 DB 업데이트 프로세스 자동화
- 서비스 안정성 확보를 위한 클라우드 인프라 최적화

타겟 사용자 접근

- 서울 디지털재단 '디지털 교육 프로그램'에 피싱지킴이 교육 과정 제안
- 노인복지관에 직접 찾아가는 '디지털 안전 교실' 운영
- 금융감독원 '전자금융 사기예방 캠페인'에 참여 제안, 앱 홍보 기회 확보

초기 자금 확보

- 한국콘텐츠진흥원 '콘텐츠 스타트업' 지원 사업 신청
- 서울시 사회적경제지원센터 '소셜벤처' 지원 프로그램 활용
- 공익목적 크라우드펀딩 진행

② 서비스 확장 및 수익 모델 강화

서비스 확장

- 공유 인텐트 활용: 모바일 OS 공유 메뉴에서 PWA 링크 연동으로 신속한 분석 환경 제공
- Smart Things 연동
- 보이스피싱 녹음 분석 기능 개발
- 앱 내 개인정보 비식별화 처리 모듈 탑재

수익 모델 구체화

- 정상 금융앱/공공앱 대상 정보 제공 및 광고 유치
- 가명처리 피싱 패턴 데이터 리포트 판매
- 학습용 비식별화 데이터셋 판매

파트너십 구축

- 금융보안원과 데이터 공유 MOU 체결
- 시중은행과 앱 내 배너 및 피싱 예방 캠페인 협력
- 시니어 대상 스마트폰 교육기관과 제휴

③ 실시간 피싱 방지 시스템 구축 (백그라운드 동작 앱)

화면 모니터링 기반 선제적 보호

- 사용자 동의 기반 화면 콘텐츠 실시간 OCR 분석 (기존 기술 활용)
- 메시지, 웹사이트, 앱 내용에서 피싱 패턴 자동 감지
- 위험 감지 시 즉시 경고 알림 표시 (화면 오버레이 방식)

프라이버시 보호 강화

- 분석은 기기 내에서 로컬 처리
- 사용자가 선택적으로 모니터링 범위 설정 가능
- 개인정보 비식별화 처리를 통한 민감 정보 보호

비즈니스 확장

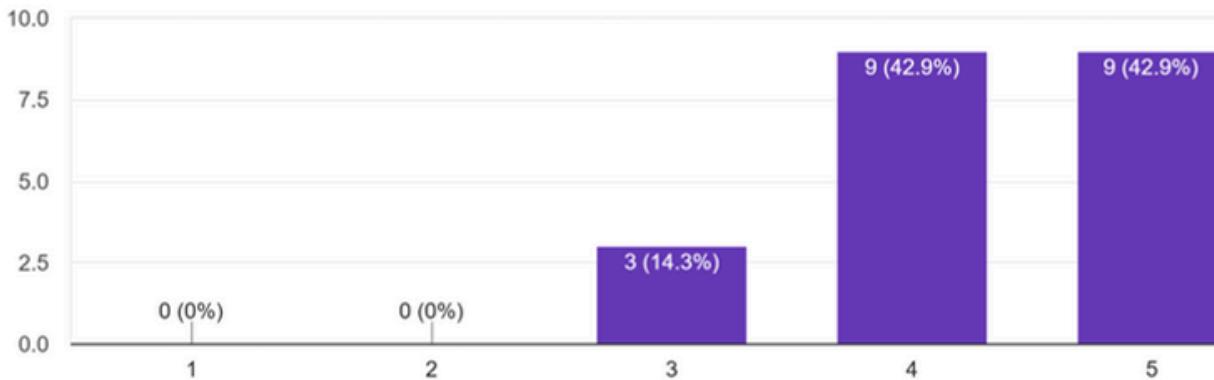
- 기업 임직원 대상 피싱 방지 서비스 패키지 출시
- 금융앱에 피싱 탐지 API 제공 (유료 서비스)
- 프리미엄 구독 서비스 출시

사용자 피드백 및 테스트

〈피싱지킴이 구글 설문조사 결과〉

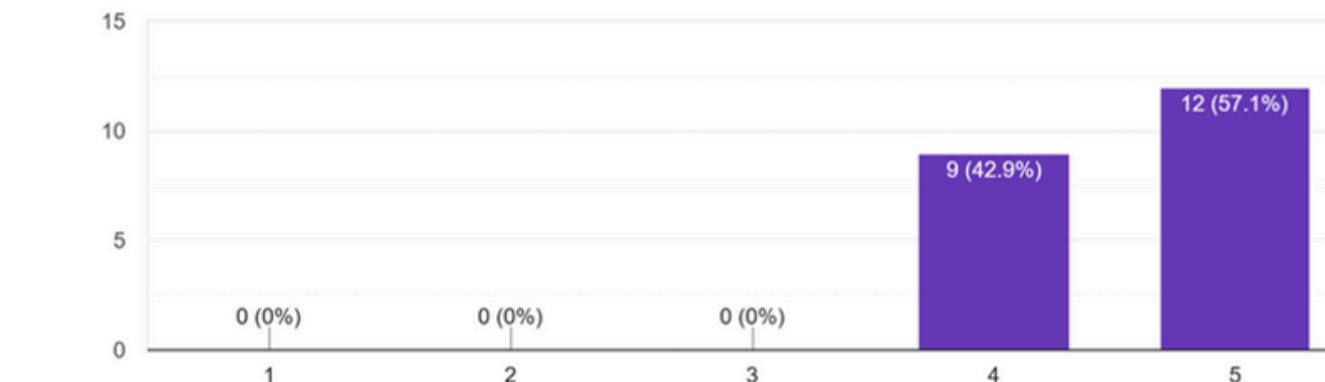
21명을 대상으로 설문조사 실시 50대 이상을 50% 비율로 설문조사 실시

4. [피싱감지] 다른 피싱감지웹/앱과 비교했을 때 피싱문자를 감지하는 데 얼마나 도움이 되셨나요? (1점 전혀 도움 안됨 - 5점 매우 도움됨)
응답 21개



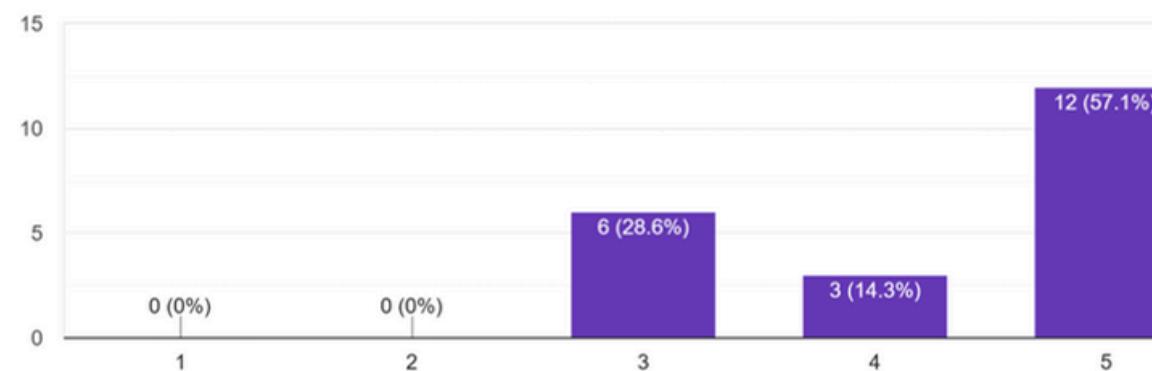
매우 도움됨(42.9%), 도움됨(42.9%), 보통(14.3%)

6. [커뮤니티] 피싱지킴이에 있는 커뮤니티 기능이 피싱정보공유를 위해 사용하실 의향이 있으신가요? (1점 전혀 없음 - 5점 매우 있음)
응답 21개



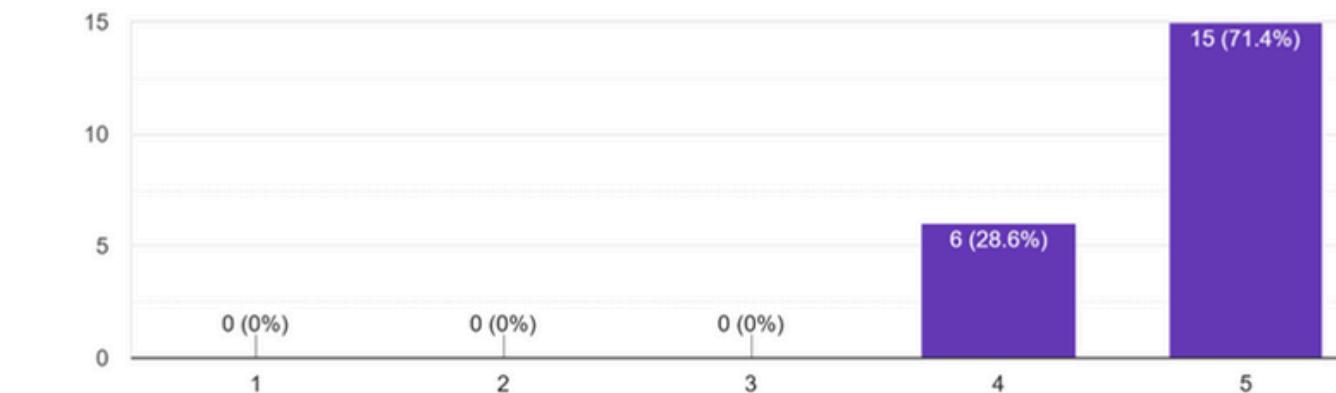
매우 있음(57.1%), 있음(42.9%)

5. [교육] 피싱지킴이에 나와있는 퀴즈와 교육자료로 피싱교육에 도움이 되셨나요? (1점 전혀 도움 안됨 - 5점 매우 도움됨)
응답 21개



매우 도움됨(57.1%), 도움됨(14.3%), 보통(28.6%)

[종합] 피싱지킴이가 생기면 이용하실 의향이 있나요? (1점 전혀 없음 - 5점 매우 있음)
응답 21개



매우 있음(71.4%), 있음(28.6%)

07

구현링크 및 스크린샷

전화번호 검사 결과

신고된 번호입니다: (총 843건 - 후후: 833건)

전화번호: 02-434-2252

이미지에서 발견된 정보

계좌번호
434-2252
[신고하기](#)

이미지 콘텐츠 분석

확인된 공식 전화번호가 없으므로 피싱 메시지 특징을 바탕으로 평가하겠습니다. 문자 메시지는 긴급성을 강조하며("즉시 문의"), 본인 확인 절차 없이 카드 발급 완료를 알리고 있습니다. 또한, 전화번호 표기가 메시지 본문과 발신번호에서 다르게 표기되어 있으며 (402.434.2252 vs 02-434-2252), 웹사이트 링크는 없지만, 전화번호를 클릭 유도하는 행위가 피싱의 전형적인 수법입니다. 전반적으로 문법 오류는 없지만, 기관 사칭(롯데카드) 의심이 강하며, 정상적인 카드 발급 절차와는 다르게 긴급성을 강조하는 점을 고려할

구현링크
: <https://phishingguard-front-pro.vercel.app/>

전체 시연 영상
: <https://www.youtube.com/watch?v=ftvPnElpUX8>

웹사이트 둘러보다가 이런 화면이 떴네요
작성자: mangoo
5일 전

그냥 평범한 게시물 보고 있는데 갑자기 다른 페이지로 이동하면서 이런 화면이 떴어요. 이거 괜찮은 건가요? 너무 무섭네요...

1 단계 : App Store에서 앱을 탭하여 무료로 설치하십시오!
2 단계 : 응용 프로그램을 열어 브라우저 속도를 높이고 수정하십시오!

지금 수리

피싱 같아요 (2) 피싱 아니에요 (0)
 저도 받았어요 (1) 피해접수 (1)

댓글 4개

영상 자료
스미싱 관련 교육 및 예방 영상

스미싱 특징
스미싱 특징 영상 1

스미싱 특징 영상 2

스마트폰 보안 설정
기기별 스미싱 예방 설정 방법

원 UI 6.0 업데이트를 지원하는 최신 갤럭시 스마트폰
해당 기능을 켜면 외부앱 설치가 차단됩니다.

원 UI 6.0 업데이트를 지원하는 최신 갤럭시 스마트폰
해당 기능을 켜면 외부앱 설치가 차단됩니다.

Q. 피싱 문자 판별

[Web발신] 홍*동님 인터넷에서 이용자비밀번호 변경.본인요청 아닐시 즉시신고요망 <1599-1111> 이 메시지는 피싱일까요?

피싱이다
피싱이 아니다

정답입니다!
정답입니다!
획득한 점수: 30점
총 점수: 360점

멜론 티켓 사칭 피싱 주의!
2일 전 · 카테고리: 피싱

멜론 티켓 사이트를 가장한 가짜 웹사이트(피싱 사이트)가 발견되었습니다. 이 사이트는 과거 콘서트 정보와 환불 문구를 이용해 사용자들을 속이고 개인 정보를 빼앗으려 합니다. 특히 봄철 공연 시즌을 노린 것으로 추정되며, 중국어 문구 등을 통해 중국발 사기로 추정됩니다. 가짜 사이트는 주소(URL)와 아이콘 등이 진짜 사이트와 다르므로 주의해야 합니다.

이는 일반 사용자들에게 봄철 공연 티켓 예매 시 피싱 사기에 주의해야 함을 의미합니다. 공식 사이트 주소를 꼼꼼히 확인하고, 의심스러운 링크는 절대 클릭하지 않도록 해야 피해를 예방할 수 있습니다. 금전 거래가 발생하는 모든 온라인 서비스에서 주의가 필요합니다.

[원문 보기](#)

1 2 3 4 5 다음 >

참고문헌

- P.Kalaharsha(2021), “Detecting Phishing Sites- An Overview”, Center of excellence in cyber security, Institute for Development and Research in Banking Technology (IDRBT), Hyderabad, India
- Akihito Nakamura(2019), “Proactive Phishing Sites Detection”, University of Aizu Aizu-Wakamatsu, Fukushima, Japan
- 김영준(2022), “URL 주요특징을 고려한 악성URL 머신러닝 탐지모델 개발”, 한국정보통신학회논문지 Vol. 26, No. 12: 1786~1793, Dec. 2022
- 금융감독원, “피싱피해시 주요 연락처”, <https://fss.or.kr/fss/main/contents.do?menuNo=200366>
- LEE JIN LEE(2015), “웹사이트 특징을 이용한 휴리스틱 피싱 탐지 방안 연구”, 정보처리학회논문지/컴퓨터 및 통신 시스템 제4권 제10호(2015. 10)
- 강현중(2014), “피싱에 대한 분석 및 대응방안에 대한 연구”, 융합보안 논문지 제14권 제5호 (2014. 09)
- 남시현 기자, 「[IT하는법] 외부 앱 설치 차단으로 스마트폰 피싱」, 『동아일보』, 2024-01-30, <https://www.donga.com/news/It/article/all/20240130/123302350/1>
- 김예지 기자, 「스팸 문자, 아이폰 기본 설정으로 간단하게 차단하자」, 『IT동아』, 2024.11.05, <https://www.donga.com/news/It/article/all/20240130/123302350/1>
- 삼성카드, “보이스피싱 피해 시 대처방법”, <https://www.samsungcard.com/personal/customer-service/provention/accident/UHPPCC0354M4.jsp>