2024 학기 말 성과 발표회

피싱 탐지 확장프로그램

개발 배경

- 2023년 한국은행 발표에 따르면 피싱사기 등 전자금융사기 피해액이 2년 사이 3배 증가했으며, 수법은 더욱 교묘해지고 있음.

- 특히 카카오뱅크, 토스 등 디지털 금융 확산으로 20-30대 젊은 층의 피해가 급증하고 있으며, 피싱 사이트의 정교함으로 인해 IT 친숙층도 피해를 입는 사례가 증가

핵심 기능

- 휴리스틱 구문분석 및 CTI를 활용한 웹사이트 안전도 분석 위험 식별 알림
- 크롬 확장프로그램을 이용한 높은 접근성
- 실시간 위험 분석 알림 제공을 통한 기능성
- 가상 이메일, 가상 전화번호 제공을 통한 개인정보 유출 방지
- 국세청 API 연동을 통한 실시간 사업자 정보 검증 시스템을 구축함

개발 내용

웹사이트 안전도 분석 시스템

- DNSBL, SSBL 연동으로 도메인 평판, 생성일자, 소유자 확인
- SSL 인증서 상태 확인 로직 구현

임시 이메일/전화번호 발급 시스템

- 임시 이메일 서버 구축 (Mailgun 활용)
- Twilio API 연동으로 가상 전화번호 서비스

그림 1. 위험요소 분석

크롬 확장프로그램 개발

- Typescript 기반의 사용자 인터페이스를 구현함.
- Background Scripts를 통한 서버 통신 및 데이터를 처리함.
- 싱글톤 패턴을 활용한 효율적인 서비스 클래스 구조를 설계함
- 모듈화된 설계로 높은 유지보수성과 테스트 용이성을 확보함

보안 및 에러 처리

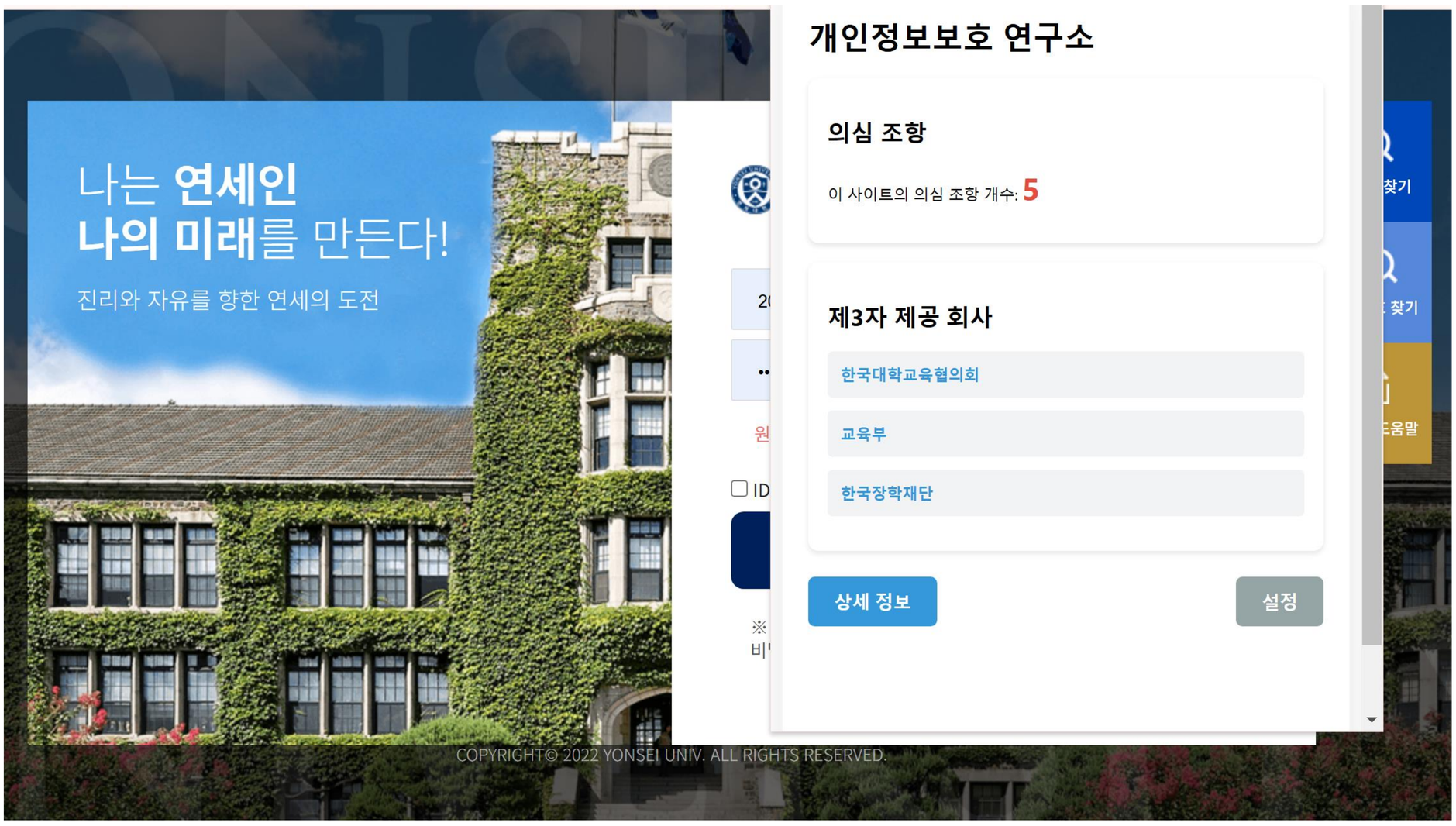
- crypto API를 활용한 보안 강화 임시 데이터 생성 시스템을 구현함
- 환경별 차별화된 로깅 전략으로 효율적인 디버깅 시스템을 구축함
- 체계적인 에러 핸들링으로 안정적인 서비스 운영을 달성함
- 민감 정보 보호를 위한 보안 메커니즘을 설계 및 구현함
  데이터 처리 및 최적화
- 24시간 캐싱 전략을 통해 불필요한 API 호출을 최소화하고 성능을 최적화함
- 재시도 메커니즘을 구현하여 네트워크 불안정 상황에서의 안정성을 확보함
- 데이터 유효성 검증 및 자동 정리를 통한 안정적인 리소스 관리를 구현함

그림 2. 피싱 감지 화면

향후 개발 계획

- 글로벌 피싱 위협 인텔리전스 통합 및 실시간 모니터링지원
- AI 기반 지능형 피싱 탐지 고도화
- 개인정보 유출 방지를 위한 선제적 보호 체계
- 개인정보 유출 사고 예방을 위한 조기 경보 시스템
- 기업 신뢰도 기반 안전성 평가 기여

본 포스터는 2024년 정보보안 해킹 소모임 Y-CERT의 연구 결과로 수행되었습니다.



테마 설정

다크 모드

알림 설정

개인정보 위험 알림 받기

개인정보 설정

1. 내 정보를 수집해서 **광고 문자나 이메일**을 보내도 괜찮아요
2. 내 정보로 **맞춤 서비스**를 제공해도 좋아요
3. **다른 회사**와 내 정보를 나눠도 괜찮아요
4. 내 **위치 정보**를 사용해도 돼요
5. 내 **사진이나 동영상**을 회사에서 써도 괜찮아요
6. 내 **구매 내역**을 분석해서 사용해도 돼요

설정 저장

피싱 위험 감지됨!

현재 접속한 사이트가 피싱 사이트로 의심됩니다. 개인정보 입력에 주의하세요.

도메인 생성일	2024-02-15 (5일전)
AI 분석 위험도	높음 (85%)
유사 도메인 탐지	네이버 피싱 의심
SSL 인증서	유효하지 않음

임시 이메일 생성하기

피싱 사이트 신고하기

security.naver-login.com

위험: 89%

도메인 정보	연관 신고
5일전 생성됨	312건
AI 분석	보안 인증
고위험	없음

임시 연락처 생성기

안전한 거래를 위한 임시 연락처를 생성하세요

임시 이메일 24시간 유효

temp_user492@secure-mail.com

복사하기

임시 전화번호 1시간 유효

+82-10-1234-5678

복사하기

수신 설정

SMS 수신 | 이메일 수신

수신 전달 | 알림 설정

새로운 임시 연락처 생성