최근 **해킹 사례**를 통해 알아보는

해킹으로 인한 개인정보 유출 사례와 대책

PRIORITY ONE
정보보안학과 20231773 김신아

개요

주제 선정 이유

디지털 환경이 발전하며 해킹으로 인한 개인정보 유출 사고가 증가하고 있습니다.
개인의 사생활 침해뿐만 아니라 기업이나 국가의 대규모 데이터 유출 사건이
연달아 발생하는 것을 보며, 보안의 중요성을 체감하게 되었습니다.

이에 최근 해킹 사례를 통해 현황을 분석하고 예방 및 대응 방안을 모색하고자 주제로 선정하게 되었습니다.

목차

최근 유출 사례

NIA 개인정보 유출 사건

2025년 2월 25일 외부인 1명에게 개인정보가 포함된 자료 파일이
유출되어 약 6,562명의 개인정보가 유출된 것으로 확인

추가 유출 방지를 위한 조치를 시행하였으며,
외부 유출된 자료를 회수하고 피해 발생 여부를 파악하기 위해
관계기관에 신고하여 추가적인 조치도 진행 중

블랙야크 개인정보 유출 사건

2025년 3월4일 해커에 의한 홈페이지 공격으로 개인정보가 포함된 자료 파일이 유출돼 약 34만2253명의 개인정보가 유출된 것으로 확인

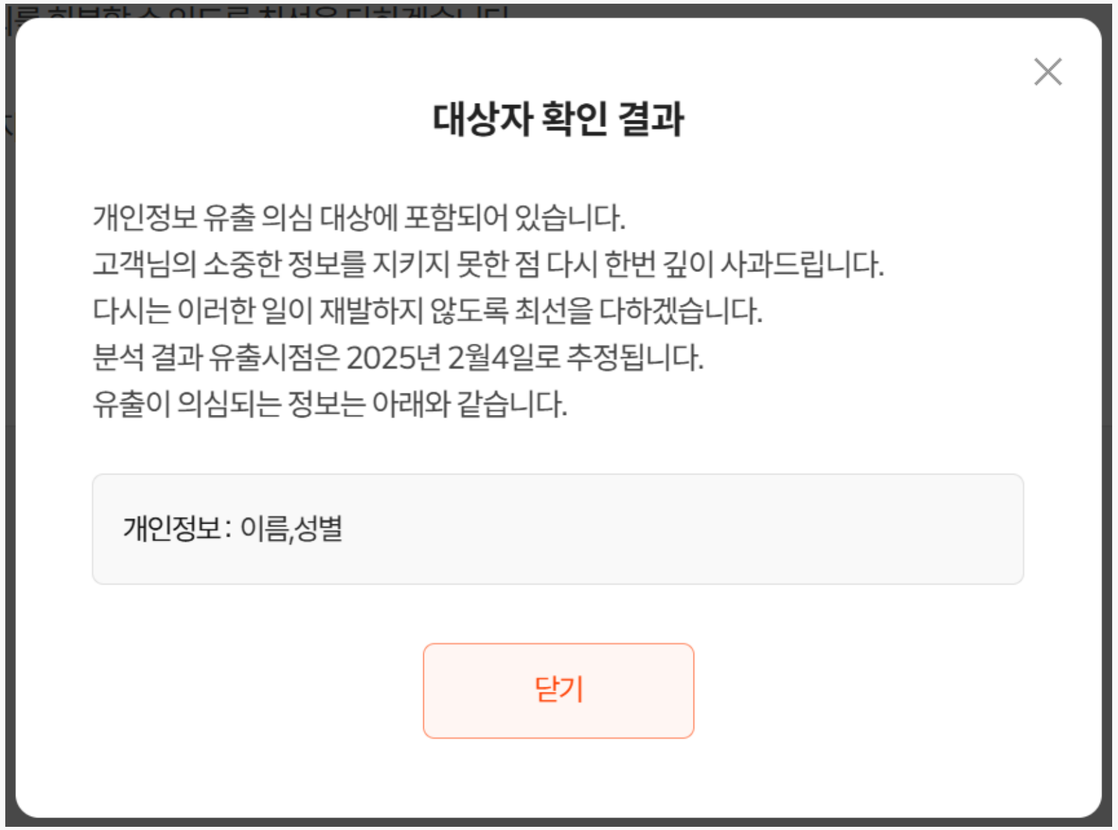
"유출 사실을 인지한 후 해커가 접속한 해당 IP와 우회 접속한 IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완 조치했다"

인크루트 개인정보 유출 사건

2025년 1월 19일부터 2025년 2월 4일까지 17일간 개인정보 유출,
유출 경위는 해커에 의한 외부 공격으로 확인

1. 관련 IP 차단 조치
2. 시스템 취약점 점검 및 보완 조치
3. 시스템 모니터링 강화 조치

인크루트 개인정보 유출 사건

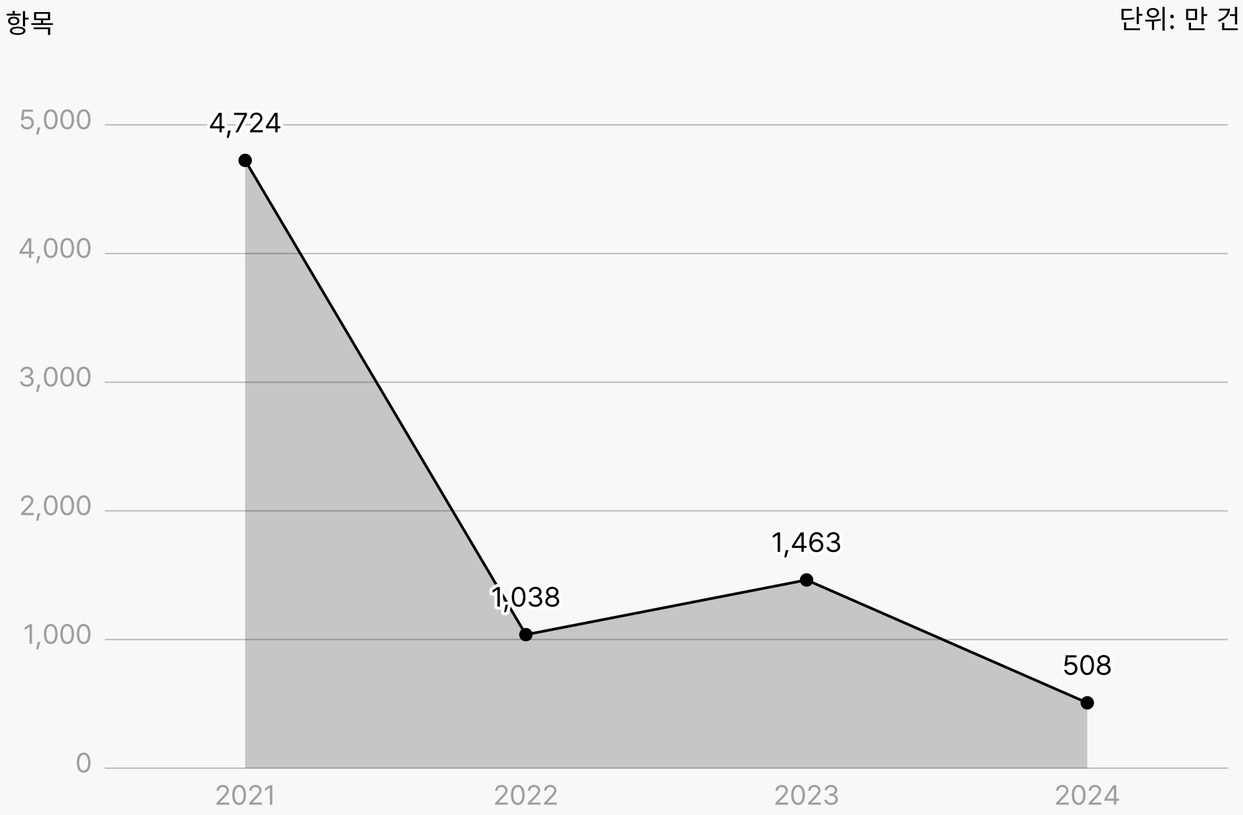


취업포털 인크루트 개인정보 유출 사고는
단순한 연락처나 기본 정보뿐만 아니라
이력서, 자기소개서, 학력, 경력, 자격증 등
민감한 정보까지 포함된 것으로 2차 피해 우려가 높다.

자소서와 이력서에는 지원자의 개인 신상이 고스란히 담겨 있어
유출될 경우 신원 도용, 맞춤형 피싱, 스팸 사기,
불법 채용 브로커 악용 등으로 이어질 위험이 크다.

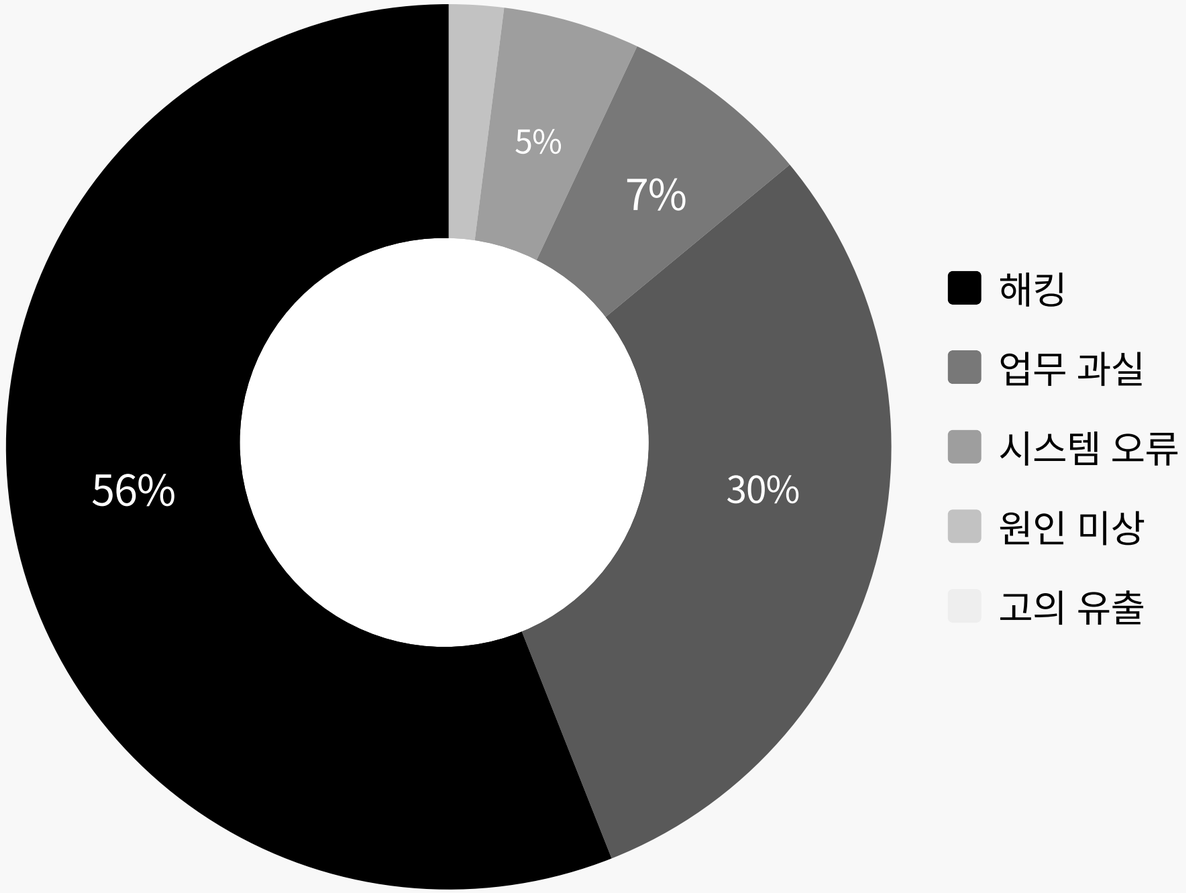
개인정보 유출 현황

개인정보 유출 규모



최근 4년간 공공기관 및 민간 개인정보유출 건수 현황[자료=강민국 국회의원실]

개인정보 유출 원인



개인 정보 유출 신고 현황과 유형
출처 : 개인정보위

주요 요인 분석

보안 솔루션 도입

이메일 보안 강화

발신자 인증, 콘텐츠 필터링,
첨부파일 검사를 통한 이메일 보안

개인정보 탐지 및 차단

자동화된 패턴 인식 시스템으로
개인정보 식별 및 차단

망분리 및 접근통제

내외부망 분리와 엄격한 접근통제로
유출 경로 차단

데이터 암호화

저장 및 전송 데이터의 엔드투엔드
암호화 적용

실시간 모니터링

24시간 이상 행동 감지 및
즉각적인 대응 체계 구축

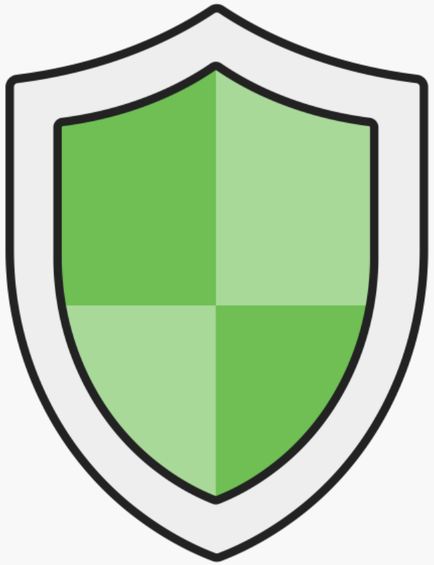
유출의 주요 요인

내부자 요인

- 직원의 부주의 또는 실수
- 악의적인 내부자 행동
- 보안 교육 부족

전송 경로 취약점

- 이메일을 통한 정보 유출
- 홈페이지 보안 취약점
- 안전하지 않은 파일 공유



접근 통제 미흡

- 과도한 시스템 접근 권한
- 미흡한 비밀번호 정책
- 불충분한 인증 절차

정책 및 절차 부재

- 명확한 보안 정책 부재
- 정기적인 보안 감사 미실시
- 사고 대응 계획 미비

업무과실에 의한 개인정보 노출/유출 사례

홈페이지 관리자 부주의

- 게시판을 통한 개인정보 공개 시,
  개인정보 비 식별화 처리 누락
- 개인정보가 포함된 게시글/댓글 게시 시,
  게시글의 비 공개 설정 누락
- 개인정보가 포함된 첨부파일 게시 시,
  첨부파일에 불필요 정보 삭제 등의 조치 미흡

이메일 오발송 & 검색엔진 노출

- 단체 메일 발송 시, "숨은 참조" 나 "개별 발송"기능을
  적용하여 수신자를 숨김 처리해야 함을 누락
- 홈페이지를 통해 노출된 개인정보가 검색엔진을 통한
  지속적 노출
- 수신 대상 메일 아이디 및 잘못된 메일 도메인에게 발송

출처 : 개인정보보호 포털

보안 대책 방안

02 기술적 보안 대책

다중 인증 시스템

- 생체 인식 기술 활용
- 모바일 인증 앱 도입
- 하드웨어 보안 키 지원

네트워크 보안 강화

- 차세대 방화벽 구축
- 침입 탐지/방지 시스템
- 암호화 통신 의무화

접근 권한 관리

- 최소 권한 원칙 적용
- 정기적 권한 검토
- 자동화된 계정 관리

보안 모니터링

- 24/7 보안 관제
- 이상 행동 탐지 시스템
- 로그 분석 및 감사

02 관리적 보안 대책

보안 교육 프로그램

모든 직원을 대상으로 한
기본 보안 교육과 개인정보
취급자를 위한 심화 교육으로
구분하여 체계적인 교육
커리큘럼을 개발하고
분기별로 실시

보안 정책 문서화 및 공유

조직의 보안 정책과 절차를
명확하게 문서화하고,
모든 직원이 쉽게 접근하고
이해할 수 있는 형태로 제공

정기적 내부 감사

분기별로 내부 보안 감사를
실시하여 정책 준수 여부를
확인하고, 개선이 필요한
영역을 식별하여
즉시 조치

보안 프로세스 강화

입사, 부서 이동, 퇴사 등
인사 변동 시 자동으로
적절한 접근 권한이 부여되고
해제되는 시스템을 구축

개인정보 유출 방지 시스템 구축

법적 규제

사고 대응 계획 수립

법률 요구사항 파악

개인정보보호법, 정보통신망법 등
관련 법규 분석 및 의무사항 식별

내부 정책 수립

법적 요구사항을 충족하는
상세한 내부 개인정보 보호
정책 및 지침 수립

정기적 감사 실시

분기별 또는 반기별 법규
준수 상태 점검 및 문서화

유출 대응 계획 수립

사고 발생 시 72시간 내 신고,
피해자 통지, 피해 최소화를 위한
단계별 대응 계획 마련

지속적인 정책 개선

법률 개정 및 새로운 보안 위협에
대응하여 정책 지속 업데이트

보안 문화 조성

보안 인식 제고 프로그램

보안 인식 기초 확립

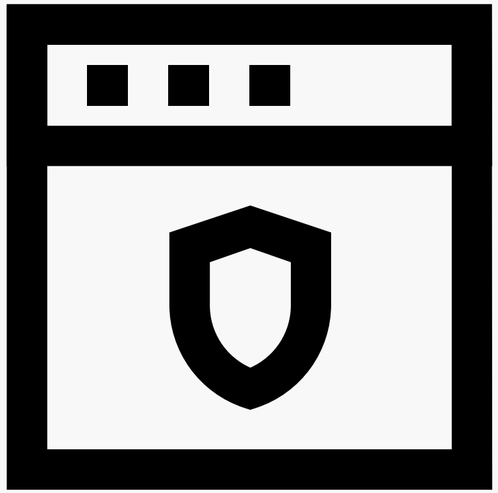
모든 직원을 대상으로 한 기본 보안 교육 제공 및
보안의 중요성에 대한 인식 형성

부서별 맞춤형 교육

각 부서의 특성과 취급하는 정보에 맞춘
심화 교육 프로그램 운영

인센티브 및 인정 제도

보안 준수 및 개선 활동에 대한 보상 체계 마련



보안 챔피언 양성

각 부서에서 보안 문화를 선도할 '보안 챔피언'
지정 및 특별 교육 제공

지속적인 훈련 및 평가

정기적인 모의 훈련, 평가, 피드백을 통한
지속적인 역량 강화

마무리

결론

보안 문화

모든 구성원이 보안을 우선시하는 조직 문화

인적 보안

교육, 인식, 책임감을 통한 인적 요소 강화

관리적 보안

정책, 절차, 감사를 통한 체계적 관리

기술적 보안

최신 보안 기술과 솔루션 구현

감사합니다!

Q & A