Leakage

개인정보, 어떻게 지켜야 하나요?

현장의 궁금증을 해결해 드립니다

글 공주영

Q

여러 대기업의 개인정보 유출 사고가 반복되면서 거주지 주소와 생활 동선 같은 사적인 정보까지 노출되는 등 피해 우려가 점점 커지고 있습니다. 개인정보를 안전하게 지킬 수 있는 구체적인 예방법과 올바른 대처 방안은 무엇인가요?

2024년 총 307건의 개인정보 유출 사고 발생

해킹	171건	56%
업무 과실	91건	30%
시스템 오류	23건	7%
고의 유출	5건	2%

A 최근 발생한 대규모 개인정보 유출 사고는 단순한 연락처를 넘어 개인의 사생활이 담긴 민감한 데이터까지 포함하고 있어 각별한 주의가 필요합니다. 산업현장에서 사고 예방을 위해 매일 안전모를 점검하듯, 디지털 세상에서도 나만의 보안수칙을 생활화하는 자세가 절실합니다.

개인정보를 지키기 위해 가장 먼저 실천해야 할 일은 로그인 보안을 강화하는 것입니다. 여러 사이트에 동일한 비밀번호를 사용하는 습관은 단 한 번의 유출로 모든 계정이 뚫리는 엄청난 결과를 초래합니다. 주요 사이트마다 비밀번호를 다르게 설정하고, 아이디와 비밀번호 외에 추가 인증을 거치는 '2단계 인증'을 활성화해야 합니다. 또한 일상 속 무심코 버리는 택배 송장 역시 유출의 원인이 될 수 있으니 반드시 파기 후 배출하도록 합시다.

만약 개인정보 유출 여부가 불안하다면 한국인터넷진흥원에서 제공하는 '털린 내 정보 찾기(kidc.eprivacy.go.kr)' 서비스를 통해 유출 이력을 수시로 점검할 수 있습니다. 명의도용 방지 서비스인 '엠세이퍼(www.msafer.or.kr)'를 활용해 나도 모르는 신규 휴대전화 개통을 원천적으로 차단할 수도 있습니다. 그리고 개인정보 포털(www.privacy.go.kr)에서는 가입한 웹사이트 현황을 확인하고 불필요한 사이트의 회원 탈퇴도 한 번에 처리할 수 있습니다.

안타깝게도 이미 유출 통보를 받았다면 신속한 사후 조치가 필수적입니다. 유출된 계정과 유사한 비밀번호를 사용하는 모든 사이트의 정보를 즉시 변경하고, 카드 정보 노출이 의심될 경우는 금융사에 연락해 재발급 및 결제 정지 조치를 진행해야 합니다.

개인정보보호위원회와 한국인터넷진흥원이 발표한 「2024년 개인정보 유출 신고 동향 및 예방 방법」에 따르면, 유출 신고의 66%가 민간기업에서 발생했다고 합니다. 원인은 해킹(56%) 외에도 게시판·SNS·채팅방 등 개인정보 파일 게시, 이메일 동보(수신자 간 정보 노출) 발송, 이메일 및 공문 내 개인정보 파일 첨부, 개인정보 파일(서류) 분실 같은 과실이 상당 부분을 차지했습니다. 따라서 사업장에서도 보안에 대한 투자와 관리 역량 강화가 반드시 필요합니다. 무엇보다 자기 스스로가 사생활 보호를 넘어 안전한 노동 환경을 유지하는 필수적인 안전 수칙으로서 보안 습관을 몸에 익혀야 합니다.

개인정보 예방 체크리스트

일상에서

- 온라인 회원 가입 시 서비스 이용에 필요한 필수 개인정보만 제공하기
- 스미싱·스팸 피해 방지를 위해 모르는 번호로 온 메시지는 클릭하지 않기
- SNS 콘텐츠에 개인정보가 포함되어 있는지 확인하기
- 공용 Wi-Fi 및 네트워크 사용 시 민감한 정보는 입력하지 말기
- 온라인상에서 결제 시 개인정보 유출 조심하기

직장에서

- 업무 관련 개인정보 수집할 경우, 최소 수집 원칙을 지키기
- 문서 공유 시 불필요한 개인정보가 포함되지 않도록 주의하기
- 업무 관련 단체방에서 자료 전송 시 개인정보 유출 주의하기
- 개인정보가 포함된 서류는 사용 후 즉시 파기하기
- 업무 관련 개인정보 법규 위반 사례는 사전에 방지하기

자료 출처

개인정보보호위원회, 한국인터넷진흥원.
「2024년 개인정보 유출 신고 동향 및 예방 방법」
공공데이터포털. 2025. 3, 4~7.
개인정보보호위원회. 내정보지킴이(mydatasafe.kr).