

개인정보 보호, 생활 속 실천과 사전 점검이 중요합니다

- 개인정보보호위원회, 국민과 기업·기관이 지켜야 할 보호수칙 안내
- 국민은 2단계 인증 활용, 명의도용 여부 주기적 확인, 의심 연락 주의
- 기업·기관은 정보자산 파악, 불필요한 서비스 등 정리, 취약점 정기 점검

최근 인공지능(AI)을 악용하여 보안 취약점을 노리는 해킹이 늘면서, 개인정보 유출과 이를 악용한 2차 피해에 대한 우려가 커지고 있다.

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’)는 국민이 일상에서 지킬 보호수칙과 유출 시 대처법, 기업·기관에 선제적 조치사항을 안내하였다.

□ 국민은 세 가지 실천수칙을 생활화하기

① 쓰지 않는 계정 정리하고 2단계 인증 활용하기

이용하지 않는 웹사이트는 가급적 탈퇴한다. 사이트·앱 로그인 시 2단계 인증을 제공하면 적극 활용하고, 사회관계망 서비스(SNS) 등에 불필요한 개인정보까지 올리지 않도록 주의하여야 한다.

※ 개인정보위 「본인확인 내역 조회 및 웹사이트 회원탈퇴 지원 서비스」 : www.privacy.go.kr

② 계정·명의도용 여부 확인하고 의심 연락 조심하기

주기적으로 「털린 내 정보 찾기」 등 공공서비스를 통해 계정정보 유출이나 명의도용 여부를 확인하는 것이 바람직하다. 특히 비밀번호가 유출됐다면 같은 비밀번호를 쓰는 다른 사이트 등의 계정도 변경하여야 한다.

낮선 문자, 전화 또는 이메일을 통해 받은 링크는 바로 누르지 말고, 공식 홈페이지나 앱을 통해 사실관계를 먼저 확인하여야 한다.

③ 피해가 의심되면 신고·상담하기

개인정보 침해는 개인정보 침해신고센터(118), 보이스피싱·스미싱은 경찰청 전기통신금융사기 통합대응단(1394), 피싱 등으로 금전적 피해가 발생했다면 경찰청(112)이나 개별 금융사 고객센터에 연락해 지급정지를 요청할 수 있다.

※ [붙임1] 일상 속 개인정보 보호수칙 포스터

[붙임2] 개인정보 보호 공공서비스 및 피해 신고·상담 문의처

□ 기업·기관은 네 가지 보호조치를 실천하기

① 관리 대상 정보자산 빠짐없이 파악하기

서버·저장장치(NAS)·네트워크 장비·단말기와 설치된 소프트웨어(버전 포함), 시스템별 처리하는 개인정보 유형, 규모, 외부와의 연계 현황* 등을 파악하여야 한다.

* 자산별 이름, 용도, 인터넷 프로토콜(IP) 주소, 운영상태, 관리책임자 등

② 쓰지 않는 서비스 정리하기

사용하지 않거나 오랫동안 방치된 홈페이지, 시스템, 계정 등은 삭제하거나 비활성화하여야 한다. 임시·시험용 시스템, 계정 등도 빠짐없이 점검하여 동일하게 조치하고, 필요 없는 외부 접속 포트는 차단하여야 한다.

③ 외부 연계 서비스와 인증정보 점검하기

외부 연계 응용프로그램 인터페이스(API) 현황을 파악하고 사용하지 않는 응용프로그램 인터페이스(API)는 폐기하여야 한다. 응용프로그램 인터페이스(API)별로 접근권한과 개인정보 조회 범위를 최소한으로 제한하고, 비정상적인 대량·반복 요청은 차단하여야 한다. 장기 미사용 응용프로그램 인터페이스(API) 키·토큰 등 인증정보는 즉시 회수하여야 한다.

④ 정기 점검하고 취약점 신속히 개선하기

앞선 조치사항들을 포함, 개인정보 보호조치는 수시로 점검하고 취약점 발견 시 신속히 개선하여야 한다. 유출사고에 대비한 대응절차와 담당체계도 미리 마련하고 상시 점검하여야 한다.

※ [붙임3] 기업·기관 사전적 개인정보 보호조치 포스터

[붙임4] 개인정보 유출 예방을 위한 API 점검사항

개인정보위 이정렬 부위원장은 “개인정보 보호는 기업·기관의 책임 있는 보호조치와 개인의 생활 속 실천이 함께하여야 한다.”라며, “개인은 보호수칙을 실천하고, 기업·기관은 취약점을 미리 점검하여 개인정보 유출과 2차 피해를 줄이는 데 힘써 주시기를 당부드린다.”라고 말했다.

담당 부서	개인정보보호위원회 사전실태점검과	책임자	과 장	김해숙 (02-2100-3060)
		담당자	사무관	유현원 (02-2100-2439)
	경찰청 전기통신금융사기 통합대응단	책임자	총 경	안동현 (02-3150-2915)
		담당자	경 정	박상현 (02-3150-0384)



일상 속 개인정보 보호수칙

1 | 쓰지 않는 계정 정리하고 2단계 인증 이용하기



- 사용하지 않는 웹사이트는 탈퇴해요
- 로그인할 때는 2단계 인증을 적극 활용해요
- SNS 등 인터넷에 불필요한 개인정보는 올리지 않아요

2 | 계정·명의도용 여부 확인하고 의심 연락 조심하기



- 공공서비스를 통해 계정정보 유출이나 명의도용 여부를 주기적으로 확인해요
- 비밀번호 유출 시, 같은 비밀번호를 쓰는 다른 사이트 등의 계정 비밀번호도 함께 변경해요
- 낯선 문자, 전화, e메일은 일단 의심해요
 - 링크를 누르거나 질문에 답하기 전에 공식 홈페이지나 앱을 통해 사실관계를 먼저 확인해요

※ 개인정보 보호 공공서비스

- **탈린 내 정보 찾기**(kdcprivacy.go.kr) : 다크웹 등에 불법 유통되는 계정정보 확인
- **본인확인 내역 조회 및 웹사이트 회원탈퇴 지원**(privacy.go.kr) : 인터넷에서 실시된 본인확인 내역 조회 및 조회된 웹사이트에 대한 탈퇴 지원
- **내 계좌 한눈에**(payinfo.or.kr) : 본인 명의의 금융계좌 및 대출 현황 등 확인
- **M-Safer**(msafer.or.kr) : 본인 명의의 통신서비스 가입 현황 확인

3 | 피해가 의심되면 신고·상담하기



- **개인정보 침해** : 개인정보 침해신고센터(118)
- **보이스피싱·스미싱** : 경찰청 전기통신금융사기 통합대응단(1394)
- **피싱 등으로 금전적 피해가 발생** : 경찰청(112) / 개별 금융사 고객센터



개인정보보호위원회

1 개인정보 보호 공공서비스

서비스명(URL)	운영기관	기능
털린 내 정보 찾기 (kidc.eprivacy.go.kr)	개인정보위	다크웹 등에서 불법 유통되는 계정정보 확인
본인확인 내역 조회 (privacy.go.kr)	개인정보위	인터넷에서 실시된 본인확인 내역 조회
웹사이트 회원탈퇴 지원 (privacy.go.kr)	개인정보위	본인확인 내역이 조회되는 웹사이트에 대한 탈퇴신청 지원
내 계좌 한눈에 (payinfo.or.kr)	금융결제원	본인 명의의 금융계좌 및 대출 현황 등 확인
금융거래 안심차단 (payinfo.or.kr)	금융결제원 / 개별 금융사	본인 명의의 계좌개설, 대출, 오픈뱅킹 거래 등 차단
개인정보 노출자 사고 예방시스템 (pd.fss.or.kr)	금융감독원	노출된 개인정보를 등록하여 이를 통한 금융 거래 시 본인확인 강화 및 일부 거래 제한
M-Safer (msafer.or.kr)	한국정보통신 진흥협회	본인 명의의 통신서비스 가입 현황 확인

2 개인정보 피해 신고·상담 문의처

상 황	문의처	전화번호/대표홈페이지
개인정보 침해에 대한 신고·상담	개인정보 침해신고센터	• (☎) 118 • privacy.kisa.or.kr
개인정보 침해로 인한 분쟁 해결	개인정보 분쟁조정위원회	• (☎) 1833-6972 • kopico.go.kr
보이스피싱·스미싱 신고 / 대응요령 확인	경찰청 전기통신금융사기 통합대응단	• (☎) 1394 • counterscam112.go.kr
보이스피싱·스미싱에 의한 금전적 피해로 긴급 지급정지가 필요한 경우	경찰청 / 해당 금융사	• (☎) 112 • (☎) 금융사별 고객센터
악성앱, 해킹 등 신고·상담	KISA 보호나라	• (☎) 118 • boho.or.kr

기업·기관 사전적 개인정보 보호조치

1 | 관리 대상 정보자산 빠짐없이 파악하기

- 다음 정보자산들의 현황을 파악해요
 - 서버, 저장장치(NAS), 네트워크 장비, 단말기(PC 등)
 - ※ 자산별 이름 / 용도 / IP주소 / 운영상태 / 관리책임자 등
 - 소프트웨어(버전 포함)
 - 시스템별 처리하는 개인정보 유형, 규모, 외부 연계 현황



2 | 쓰지 않는 서비스와 외부 노출 정리하기

- 사용하지 않거나 오랫동안 방치된 홈페이지, 시스템, 계정 등은 삭제·비활성화 해요
 - ※ 임시·시험용 시스템, 계정 등도 빠짐없이 점검해요
- 필요 없어진 외부 접속 포트는 차단해요



3 | 외부 연계 서비스와 인증정보 점검하기

- 외부 연계 API 현황을 파악하고 사용하지 않는 API는 폐기해요
- API별 접근권한과 개인정보 조회 범위를 최소로 제한하고, 비정상적인 대량·반복 요청은 차단해요
- 장기 미사용 API키, 토큰 등 인증정보는 즉시 회수해요

※ (참고) 개인정보 유출 예방을 위한 API 권한 관리 점검사항



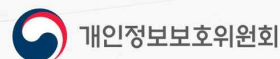
4 | 정기 점검하고 취약점 신속히 개선하기

- 앞선 조치들을 포함하여, 개인정보 보호조치는 수시로 점검해요
- 점검 과정에서 취약점을 발견하면 신속히 개선해요
- 유출사고에 대비한 대응절차와 담당체계도 미리 마련하고 상시 점검해요



개인정보보호위원회

개인정보 유출 예방을 위한



API 권한 관리 점검사항

1 개인정보 최소화

API가 반환하는 개인정보 항목과 제공 규모를 줄입니다.



필요한 데이터만 응답

화면에 보여주지 않거나
목적에 필요 없는 개인정보는
API 응답 데이터에서 제외

대량조화·응답량 제한

계정, IP, 자격증명 등을 기준으로
반복 호출, 대량 검색 등에 제한을 두어
대규모 개인정보 조화·유출 등 방지

2 최소 권한 기반 접근통제

허용된 주체·기능·범위만 개인정보에 접근하도록 합니다.



접근범위 분리

이용자, 취급자, 고객센터 등
주체별로 사용 가능한 API 및
개인정보 항목을 필요 최소한의
범위로 차등 부여

기본 차단

로그인 여부만 확인하는
것으로는 충분하지 않으며,
권한 정책을 따르지 않는
비정상 요청은 기본적으로 차단

서버 권한검사

이용자 화면에서
보이지 않는 것만으로는
충분하지 않으며, 서버에서 요청
데이터에 대한 접속 권한 확인

3 운영 API 지속 점검

운영 현황, 자격증명, 접속기록을 주기적으로 확인합니다.



오래된 API 관리

서비스 개편,
기능 종료 후 남아 있는
구버전·미사용 API
차단 또는 폐기

자격증명 회수

장기 미사용
API 카·토큰 등
자격증명 및 권한
정기적으로 점검 및 회수

이상징후 대응

접속기록을 점검하고
대량조화·반복 실패, 새벽시간 등
업무 외 시간 접속, 외국 등에서의
접속 등 비정상 패턴 탐지