ASIAN AMERICANS ADVANCING JUSTICE AAJC

2026 년 디지털 보안 도구 구축 가이드

01 전화, 문자, 이메일 서비스를 현명하게 사용하기

법 집행 기관이 통화 및 문자 기록에 접근하는 것을 방지하려면, 개인 전화번호와 연결되지 않은 종단 간 암호화기능이 있는 시그널 (SIGNAL) 또는 허시드(HUSHED)와 같은 앱을 사용하세요.

카카오톡과 텔레그램에서도 “비밀 채팅” 기능을 켜면 종단 간 암호화를 활성화할 수 있습니다.

민감한 문서를 보낼 때는 개인 이메일 주소와 연결되지 않은 별도의 이메일 계정을 만드는 것이 좋습니다.

일부 이메일 서비스 제공업체는 데이터를 광고업체나 법 집행 기관과 공유할 수 있습니다. 다음과 같은 문구에 주의하세요.

“우리는 협력 업체와 데이터를 공유할 수 있습니다” 또는
“우리는 서비스 개선을 위해 이메일을 분석합니다”

02 소셜 미디어 모범 사용 수칙을 따르기

게시물, 친구 목록, 위치 정보 등을 볼 수 있는 사람을 제한하기 위해 계정을 비공개로 설정하세요. 자동 위치 추적을 끄고, 생일이나 직장 위치 같은 개인 정보를 공유하는 것을 자제하세요.

03 온라인 추적과 맞춤형 광고 제한하기

당신은 미국 국토안보부로부터 자진 출국관련 광고를 받고 있습니까? 다른 사람보다 더 높은 가격의 제품 광고를 보고 있습니까? 당신은 맞춤형 광고의 타겟이 되고 있습니다.

소셜 미디어에서 맞춤형 광고 비활성화시키고, 휴대폰의 모바일 광고 아이디 비활성화하고, 앱의 위치 권한 제거하고, 그리고 항상 “모든 쿠키 거부”를 선택하세요. 병원, 법률 사무소, 시위 장소 등을 방문할 때는 위치 서비스 기능을 항상 꺼 두세요.

04 여행하거나 민감한 활동에 참여할 때 디지털 보안 실천하기

목적지까지 이동할 때 내비게이션이 필요하다면 인터넷 연결 없이 작동하는 오프라인 지도 앱을 사용하세요.

자동 번호판 인식 시스템 이 당신의 차량 이동을 주 경계를 넘어 추적할 수 있음을 유의하세요. 대중교통이나 택시 이용을 고려하세요.

얼굴 인식 기능과 지문 인식 기능을 꺼 두세요. 만일 휴대폰이 압수될 경우 법 집행 기관은 이러한 생체 인식을 사용해 잠금을 해제할 수 있지만 비밀번호로 잠긴 경우에는 해제할 수 없습니다.

국경에서는 개인 정보 보호 권한이 국경 순찰 요원의 재량에 따라 제한될 수 있습니다

여행 계획을 세울 때는 현재 정치적 상황과 최근 뉴스 흐름을 고려하세요

05 AI 챗봇을 신중하고 제한적으로 사용하기

이름, 주소, 사건 관련 정보, 이민 신분, 또는 개인을 식별할 수 있는 정보와 같은 개인정보를 AI 챗봇에 절대 입력하지 마세요.

대화 기록은 저장되며 향후 AI 모델을 학습시키는 데 사용될 수 있습니다.

“저는 미등록 이민자인데 미국 이민세관단속국이 집에 오면 제 권리가 무엇인지 알고 싶습니다.” **대신에**

“미국 이민세관단속국의 단속 상황에서 이민자들이 일반적으로 가지는 권리는 무엇인가요?” **라고 챗지피티에게 질문하세요.**

06 감시 카메라 및 스마트 홈 기기 사용 시 주의하기

스마트 홈 기기는 사용자가 모르게 무단 사용자나 법 집행 기관이 민감한 영상, 녹음, 또는 기기 제어 기능에 접근할 수 있는 가능성을 만들 수 있습니다.

누가 카메라와 스마트 스피커에 접근권한이 있는지 주기적으로 기기 권한 설정을 확인하고 필요하다면 스마트 홈 기기를 완전히 제거하는 것도 고려하세요.

07 공공장소에서 개인정보 보호에 유의하기

정부 건물, 대중교통 시설, 쇼핑 지역, 국경 지역과 같은 공공장소에는 감시 시스템이 매우 널리 설치되어 있습니다. 감시 카메라, 번호판 인식 장치, 얼굴 인식 기술, 그리고 심지어 주변의 무선 네트워크까지도 법 집행 기관이 개인을 식별하는 데 사용될 수 있다는 점에 유의하세요.

미국 이민세관단속국은이민 단속을 신속하게 진행하기 위해 얼굴 인식 앱들을 사용하고 있습니다.

만약 당신이 위험도가 높은 상황에 처해 있다면 마스크와 모자를 착용하고, 사용하지 않을 때는 블루투스와 와이파이를 끄고, 온라인에 게시할 사진을 촬영할 만한 사람들과 거리를 두세요.