ASIAN AMERICANS ADVANCING JUSTICE AAJC

CẨM NANG BẢO MẬT KỸ THUẬT SỐ NĂM 2026

HƯỚNG DẪN XÂY DỰNG

01 HÃY SỬ DỤNG CÁC CUỘC GỌI ĐIỆN THOẠI, TIN NHẮN VÀ EMAIL MỘT CÁCH KHÔN NGOAN

Để tránh cơ quan thực thi pháp luật truy cập vào lịch sử cuộc gọi và tin nhắn, hãy sử dụng các ứng dụng như Signal hoặc Hushed, là những ứng dụng không được kết nối với số điện thoại cá nhân của quý vị và có tính năng mã hóa đầu cuối (E2EE).

Quý vị có thể bật mã hóa đầu cuối (E2EE) trên Kakao Talk và Telegram bằng cách bật chế độ "Trò chuyện bí mật" (Secret Chats).

Hãy tạo một tài khoản email phụ, không liên kết với địa chỉ email cá nhân của quý vị khi gửi các tài liệu nhạy cảm.

Một số nhà cung cấp dịch vụ email có thể chia sẻ thông tin của quý vị với các nhà quảng cáo hoặc cơ quan thực thi pháp luật. Hãy cảnh giác với những cụm từ như:

"Chúng tôi có thể chia sẻ thông tin với các đối tác" hoặc"
"Chúng tôi quét email để cải thiện dịch vụ."

02 HÃY SỬ DỤNG MẠNG XÃ HỘI THEO CÁCH AN TOÀN

Hãy chuyển tài khoản của quý vị sang chế độ riêng tư để giới hạn người nào có thể xem bài viết, danh sách bạn bè và vị trí của quý vị. Tắt tính năng tự động theo dõi vị trí và tránh chia sẻ thông tin cá nhân như ngày sinh hoặc địa điểm làm việc.

Những diễn biến gần đây trong chính sách của Bộ An ninh Nội địa (DHS) cho phép các nhân viên thực thi pháp luật về nhập cư xem xét hoạt động trên mạng xã hội của quý vị từ 5 năm trước.

03 HÃY HẠN CHẾ SỰ THEO DÕI TRỰC TUYẾN VÀ QUẢNG CÁO NHẮM MỤC TIÊU

Quý vị có đang nhận được quảng cáo từ DHS về việc tự nguyện trục xuất không? Hay quý vị thấy giá sản phẩm hiển thị cao hơn so với giá người khác thấy? Đó là do quý vị đang bị nhắm mục tiêu để quảng cáo.

Hãy từ chối các quảng cáo được cá nhân hóa trên mạng xã hội, tắt nhận dạng quảng cáo trên điện thoại, xóa quyền truy cập vị trí cho các ứng dụng và luôn chọn "từ chối tất cả cookie". Luôn tắt dịch vụ định vị khi đến các phòng khám sức khỏe, văn phòng luật sư hoặc các cuộc biểu tình.

04 HÃY THỰC HÀNH AN NINH MẠNG KHI ĐI DI CHUYỂN HOẶC THAM GIA CÁC HOẠT ĐỘNG NHẠY CẢM

Nếu quý vị cần sử dụng định vị để dẫn đường, hãy sử dụng các ứng dụng ngoại tuyến có thể hoạt động mà không cần kết nối internet.

Hãy lưu ý rằng các thiết bị đọc biển số tự động (ALPR) có thể theo dõi hành trình của xe quý vị xuyên bang; hãy cân nhắc sử dụng phương tiện giao thông công cộng hoặc taxi thay thế.

Tắt tính năng nhận diện khuôn mặt và quét vân tay — nếu điện thoại của quý vị bị tịch thu, cơ quan thực thi pháp luật có thể sử dụng các tính năng này để mở khóa điện thoại của quý vị, nhưng không thể dùng mã PIN để mở.

Nhìn chung, việc bảo vệ quyền riêng tư phụ thuộc vào quyền tự quyết của các nhân viên tuần tra tại biên giới.

Hãy cân nhắc tình hình chính trị và tin tức mới nhất để đánh giá rủi ro cho cá nhân khi di chuyển.

05 HÃY SỬ DỤNG CHATBOT AI MỘT CÁCH THẬN TRỌNG VÀ CÓ GIỚI HẠN

Tuyệt đối không cung cấp thông tin cá nhân, chẳng hạn như tên, địa chỉ, chi tiết vụ việc, tình trạng nhập cư hoặc thông tin nhận dạng cho Chatbot AI.

Lịch sử trò chuyện sẽ được lưu trữ và có thể được sử dụng để huấn luyện các mô hình trong tương lai.

Thay vì hỏi: "Tôi là người nhập cư bất hợp pháp và cần biết quyền của mình nếu ICE đến nhà."

Hãy hỏi ChatGPT: "Các quyền cơ bản của người nhập cư khi gặp ICE là gì?"

06 HÃY THẬN TRỌNG TRONG VIỆC SỬ DỤNG CAMERA GIÁM SÁT VÀ THIẾT BỊ NHÀ THÔNG MINH

Các thiết bị nhà thông minh có thể cho phép người dùng trái phép và cơ quan thực thi pháp luật truy cập vào các đoạn phim nhạy cảm, bản ghi âm hoặc quyền điều khiển thiết bị mà quý vị không hề hay biết.

Thường xuyên kiểm tra quyền truy cập của thiết bị để xem ai có quyền truy cập vào camera và loa thông minh của quý vị, hoặc xem xét gỡ bỏ hoàn toàn các thiết bị nhà thông minh.

07 HÃY LƯU Ý VỀ QUYỀN RIÊNG TƯ Ở NHỮNG NƠI CÔNG CỘNG

Việc giám sát rất phổ biến ở những khu vực công cộng như các tòa nhà chính phủ, trạm xe, khu mua sắm và khu vực biên giới. Hãy lưu ý rằng camera giám sát, thiết bị đọc biển số xe, công nghệ nhận diện khuôn mặt, và thậm chí cả các mạng không dây gần đó đều có thể được cơ quan thực thi pháp luật sử dụng để nhận dạng quý vị.

Cơ quan ICE đang sử dụng các ứng dụng nhận diện khuôn mặt để đẩy nhanh quá trình bắt giữ người nhập cư.

Cần lưu ý rằng các công cụ này có độ chính xác thấp hơn khi nhận diện khuôn mặt người châu Á, có thể dẫn đến việc bắt giữ oan sai.

Nếu quý vị đang ở trong tình huống rủi ro cao, hãy cân nhắc việc đeo khẩu trang và nón, tắt Bluetooth và WiFi khi không sử dụng, và tránh xa những người có thể đang chụp ảnh để đăng lên mạng.