ASIAN AMERICANS ADVANCING JUSTICE AAJC

คู่มือปี 2026 สำหรับการสร้าง
ชุดเครื่องมือป้องกันภัยทางดิจิทัลของคุณ

01 การใช้โทรศัพท์, การส่งข้อความ และการใช้อีเมลอย่างรอบคอบ

เพื่อป้องกันเจ้าหน้าที่บังคับใช้กฎหมายเข้าถึงประวัติการโทรและข้อความของคุณ ควรใช้แอป Signal หรือ Hushed ที่ไม่ได้เชื่อมต่อกับหมายเลขโทรศัพท์ส่วนตัวของคุณ และมีระบบเข้ารหัสแบบต้นทางถึงปลายทาง (E2EE).

คุณสามารถใช้งานการเข้ารหัสแบบปลายทาง (E2EE) บน Kakao Talk และ Telegram โดยการเปิดโหมด “แชตลับ”

สร้างบัญชีอีเมลสำรองที่ไม่เชื่อมโยงกับอีเมลส่วนตัวของคุณ เมื่อส่งเอกสารสำคัญ

ผู้ให้บริการอีเมลบางรายอาจแบ่งปันข้อมูลของคุณกับผู้โฆษณาหรือเจ้าหน้าที่บังคับใช้กฎหมาย ระวังข้อความที่มีลักษณะเช่น:

เราอาจแบ่งปันข้อมูลกับบริษัทที่ทำงานร่วมกัน
เราแสกนอีเมลเพื่อปรับปรุงการให้บริการของเรา

02 แนวทางปฏิบัติที่ดีที่สุดในการใช้โซเชียลมีเดีย

ตั้งค่าบัญชีของคุณเป็นแบบส่วนตัวเพื่อจำกัดผู้ที่สามารถเห็นโพสต์ เพื่อน และตำแหน่งที่ตั้งของคุณ ปิดการติดตามสถานที่อัตโนมัติ และหลีกเลี่ยงการแบ่งปันข้อมูลส่วนตัว เช่น วันเกิด หรือสถานที่ทำงาน

ความคืบหน้าล่าสุดในนโยบายของกระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) อนุญาตให้เจ้าหน้าที่ตรวจคนเข้าเมืองสามารถตรวจสอบกิจกรรมโซเชียลมีเดียของคุณ 5 ปีย้อนหลัง

03 จำกัดการติดตามออนไลน์และการโฆษณาที่เฉพาะกลุ่มเป้าหมาย

คุณกำลังได้รับโฆษณาจากกระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) เกี่ยวกับการส่งตัวกลับด้วยตัวเองหรือไม่? เห็นราคาสินค้าที่สูงกว่าที่คนอื่นเห็นหรือเปล่า? คุณกำลังเริ่มเป็นเป้าหมาย

ปิดการรับโฆษณาแบบปรับตามความสนใจบนโซเชียลมีเดีย ปิดการใช้งานรหัสโฆษณาบนโทรศัพท์มือถือของคุณ ลบสิทธิ์ในการอนุญาตเข้าถึงตำแหน่งของแอป และคลิก ‘ปฏิเสธคุกกี้ทั้งหมด ’เสมอ ปิดบริการตำแหน่งเสมอเมื่อไปคลินิกสุขภาพ สำนักงานกฎหมาย หรือการชุมนุมประท้วง

04 การปฏิบัติด้านความปลอดภัยดิจิทัลเมื่อเดินทางหรือเข้าร่วมกิจกรรมที่มีความละเอียดอ่อน

หากคุณต้องใช้ระบบการนำทางเพื่อไปยังจุดหมาย ใช้แอปนำทางแบบออฟไลน์ที่ทำงานได้โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต

ระวังเครื่องอ่านป้ายทะเบียนอัตโนมัติ (ALPR) สามารถติดตามการเคลื่อนไหวของรถคุณข้ามรัฐได้ พิจารณาใช้ระบบขนส่งสาธารณะหรือแท็กซี่แทน

ปิดการใช้งานการจดจำใบหน้า และการสแกนลายนิ้วมือ—หากโทรศัพท์ของคุณถูกยึด เจ้าหน้าที่บังคับใช้กฎหมายสามารถใช้วิธีเหล่านี้ปลดล็อกโทรศัพท์ได้ แต่ไม่สามารถปลดล็อกรหัส PIN ของคุณ

การคุ้มครองความเป็นส่วนตัวโดยทั่วไปขึ้นอยู่กับดุลยพินิจของเจ้าหน้าที่ตรวจคนเข้าเมืองที่ชายแดน

พิจารณาบรรยากาศทางการเมืองและข่าวสารปัจจุบันเมื่อต้องประเมินความเสี่ยงส่วนตัวในการเดินทาง

05 ใช้แชตบอท AI อย่างรอบคอบและจำกัด

อย่าใส่ข้อมูลส่วนตัว เช่น ชื่อ ที่อยู่ รายละเอียดคดี สถานะการเข้าเมือง หรือข้อมูลที่สามารถระบุตัวตน ลงในแชตบอท AI

ประวัติการสนทนาจะถูกเก็บไว้ และสามารถถูกนำไปใช้ฝึกสอนโมเดล AI ในอนาคต

แทนที่จะใช้ข้อความว่า ฉันไม่มีเอกสารและต้องการทราบสิทธิของฉันถ้า ICE มาที่บ้าน

ถาม ChatGPT: ‘สิทธิทั่วไปของผู้อพยพระหว่างการเผชิญหน้ากับเจ้าหน้าที่ ICE ?

06 ใช้กล้องวงจรปิดและอุปกรณ์สมาร์ทโฮมอย่างระมัดระวัง

อุปกรณ์สมาร์ทโฮมอาจอนุญาตให้ผู้ใช้ที่ไม่ได้รับอนุญาตและเจ้าหน้าที่บังคับใช้กฎหมายเข้าถึงภาพวิดีโอ ข้อมูลที่บันทึก หรือการควบคุมอุปกรณ์ที่ละเอียดอ่อนได้โดยที่คุณไม่รู้ตัว

ตรวจสอบการอนุญาตการเข้าถึงอุปกรณ์ของคุณเป็นประจำเพื่อดูว่าใครสามารถเข้าถึงกล้องและลำโพงอัจฉริยะได้ หรือพิจารณาลบอุปกรณ์สมาร์ทโฮมออกทั้งหมด

07 คำนึงถึงความเป็นส่วนตัวในพื้นที่สาธารณะ

มีการตรวจตรสอย่างกว้างขวางในพื้นที่สาธารณะ เช่น อาคารรัฐบาล สถานีขนส่ง ย่านการค้า และเขตชายแดน ระวังกล้องวงจรปิด เครื่องอ่านป้ายทะเบียน เทคโนโลยีจดจำใบหน้า และแม้แต่เครือข่ายไร้สายใกล้เคียง อาจถูกเจ้าหน้าที่บังคับใช้กฎหมายใช้เพื่อระบุตัวตนคุณได้

ICE ใช้แอปจดจำใบหน้าเพื่อเร่งกระบวนการจับกุมคนเข้าเมืองเร็วขึ้น

โปรดระวังว่าเครื่องมือนี้มีความแม่นยำน้อยกว่ากับใบหน้าของคนเอเชีย ซึ่งอาจทำให้เกิดการจับกุมที่ผิดพลาดได้

หากคุณอยู่ในสถานการณ์ที่มีความเสี่ยงสูง ควรสวมหน้ากากและหมวก ปิดบลูทูธ และ WiFi เมื่อไม่ได้ใช้งาน และหลีกเลี่ยงผู้คนที่อาจถ่ายภาพเพื่อนำไปโพสต์ออนไลน์