ASIAN AMERICANS ADVANCING JUSTICE AAJC

GABAY PARA PAGBUO NG IYONG DIGITAL DEFENSE TOOKLIT PARA SA 2026

DIGITAL DEFENSE TOOLKIT

01 GAMITIN ANG MGA PAGTAWAG, TEXT, AT EMAIL NANG MAY KARUNUNGAN

Upang maiwasan na ma-access ng mga alagad ng batas ang iyong historya ng tawag at text, gumamit ng mga app tulad ng Signal o Hushed na hindi nakakonekta sa iyong personal na numero at may **End-to-End Encryption (E2EE)**.

Maaari mong paganahin ang end to end sa KaKao Talk at Telegram sa pamamagitan ng pag-on ng “Secret Chats.

Gumawa ng **pangalawang email account** na hindi nakakonekta sa iyong personal na email address kapag nagpapadala ng mga sensitibong dokumento.

May ilang email provider na maaaring ibahagi ang iyong data sa mga adbertayser o alagad ng batas. Mag-ingat sa mga kataga na tulad ng:

“Maaari kaming magbahagi ng data sa mga partner” o
“Sini-scan namin ang mga email upang mapabuti ang aming mga serbisyo.”

02 GAMITIN ANG MGA PINAKAMAHUSAY NA KASANAYAN SA SOCIAL MEDIA

Gawing pribado ang iyong mga account upang limitahan ang mga nakakakita ng iyong posts, friends, at lokasyon. Huwag paganahin ang awtomatikong **pagsubaybay sa lokasyon at iwasan ang pagbabahagi ng sariling impormasyon tulad ng mga kaarawan o lugar ng trabaho.**

Sa mga bagong polisiya ng DHS, pinapayagan na ang mga immigration officer na suriin ang iyong aktibidad sa social media hanggang sa nakalipas na 5 taon.

03 LIMITAHAN ANG PAGSUBAYBAY SA ONLINE AT NAKA-TARGET NA ADVERTISING

Nakatatanggap ka ba ng mga ads mula sa DHS tungkol sa self-deportation? Nakakakita ka ba ng mga presyo ng produkto na mas mataas kaysa sa nakikita ng iba? Ibig sabihin, ikaw ay "tinatarget"

Mag-opt out ng mga personalized na ads sa social media, huwag paganahin ang mobile ad ID sa iyong telepono, alisin ang mga pahintulot sa lokasyon para sa iyong mga app, at palaging i-click ang “reject all cookies.” **Palaging i-off ang mga serbisyo sa lokasyon kapag bumibisita sa mga klinika sa kalusugan, opisina ng abogado, o mga protesta.**

04 UGALIING MAGING LIGTAS SA DIGITAL SECURITY KAPAG NAGLALAKBAY O NAKIKILAHOK SA MGA SENSITIBONG AKTIBIDAD

Kung kailangan mong gumamit ng nabigasyon upang maabot ang iyong patutunguhan, gumamit ng mga offline na app na gumagana kahit walang koneksyon sa internet.

Tandaan na ang mga **automatic license plate reader (ALPR) ay maaaring sumubaybay sa galaw ng iyong sasakyan sa pagtawid sa mga border ng estado**; sa halip isaalang-alang ang pampublikong transportasyon o mga taxi.

I-off ang Face ID at fingerprint scanning—kung makumpiska ang iyong telepono, magagamit ito ng mga awtoridad upang i-unlock ang iyong telepono, ngunit hindi nila magagamit ang iyong PIN code.

Ang mga proteksyon sa privacy ay karaniwang nakadepende sa desisyon ng mga border patrol agent.

Isaalang-alang ang sitwasyong politikal at ang mga balita sa kasalukuyan kapag tinatansya ang panganib sa iyong paglalakbay.

05 GAMITIN ANG MGA AI CHATBOT NANG MAINGAT AT MADALANG

Huwag kailanman ilagay ang sariling impormasyon, gaya ng iyong pangalan, tirahan, mga detalye ng kaso, estado ng pag-iimigrasyon, o ano mang pagkakakilanlan sa AI chatbot.

Ang kasaysayan ng chat ay naka-imbak at maaaring magamit upang sanayin ang mga modelo sa hinaharap.

Sa halip na sabihing: “Ako ay hindi dokumentado at kailangan kong malaman ang aking mga karapatan kung”. darating ang ICE sa aking pintuan.
Itanong sa ChatGPT: “Ano ang mga pangkalahatang karapatan ng mga imigrante kapag may nakaharap na opisyal ng ICE?"

06 GAMITIN ANG MGA SURVEILLANCE CAMERA AT SMART HOME DEVICE NANG MAY PAG-IINGAT.

Ang mga smart home device ay maaaring magbigay-daan sa mga hindi awtorisadong user at alagad ng batas na ma-access ang sensitibong footage, recording, o kontrol ng device nang hindi mo nalalaman.

Regular na suriin ang device permissions upang makita kung sino ang may access sa iyong mga camera at smart speaker, o isaalang-alang na tuluyan nang alisin ang mga smart home device.

07 ISAALANG-ALANG ANG IYONG PRIVACY SA MGA PAMPUBLIKONG LUGAR

Laganap ang pagsubaybay sa mga pampublikong lugar tulad ng mga gusali ng gobyerno, mga Estasyon, mga distrito ng pamilihan, at mga border zone. Tandaan na ang mga surveillance camera, mga mambabasa ng plaka ng lisensya facial recognition technology, at maging ang mga kalapit na wireless network ay maaaring gamitin ng mga tagapagpatupad ng batas upang kilalanin ka.

Gumagamit ang ICE ng mga facial recognition app para mapabilis ang kanilang mga pag-aresto na kaugnay sa imigrasyon.
Maging babala na ang mga tool na ito ay hindi gaanong tumpak sa mga mukhang Asyano, na maaaring humantong sa maling pag-aresto.

Kung ikaw ay nasa mataas na panganib na sitwasyon, isaalang-alang ang pagsusuot ng takip sa mukha at sumbrero, i-off ang bluetooth at wifi kapag hindi ginagamit, at pag-iwas sa mga taong maaaring kumukuha ng mga larawan para i-post online.