Travel & Flight Security

ACTIVIST CHECKLIST

Last updated on **March 23, 2026** Takes about **30 minutes**

Citizens can refuse to unlock a phone at the US border but the device may be detained. Visa holders and visitors who refuse can be denied entry. Power your phone off before security, use a long random passcode, disable biometric unlock, and bring paper documents so you can keep the device off through customs. Higher-risk travelers should consider a secondary phone with minimal data.

Who this checklist is for:

- ✅ Anyone traveling **internationally** crossing the US border to enter or re-enter the country (whether by land, air, or sea).
- ✅ This checklist may also be applicable for **domestic** air travel within the US as you may be at increased risk of search and adverse consequences (especially if you are not a US citizen).
- ❌ This checklist is **NOT designed for people in the US who don't have US citizenship and are at risk of deportation.** If you need advice for flying as an immigrant with varying documentation statuses, see these resources: Immigrants Rising, National Immigration Law Center

While we recommend the steps below for both entering and exiting the US, you are under much more scrutiny while ***entering the US***, so that is the time to be most cautious. If you're only going to follow these steps once, make sure it is when you enter the US.

We recommend completing the Security Essentials checklist as well.

ICE at airports: As of July 2026, ICE appears to be detaining more people at airports, including people with open asylum cases. A few examples: Someone with a valid visa and an open asylum case while boarding the plane in Denver, a failed detention in Las Vegas, and two detentions in Boston.

Short version of this guide

Either bring a secondary phone, backup and factory reset your device, or wipe everything sensitive off your device before you travel. Keep your phone off, disable biometrics, use a randomly generated passcode. Learn your rights. If you're not a US citizen and trying to enter the US, consider hiding your social media profiles before you apply for a visa. If higher risk, get a legal team and have a check-in plan with trusted contacts.

Baseline protections

EVERYONE This section is for anyone doing activism or advocacy work.

Most of the device searches we've heard of involved border police manually browsing a phone looking for things they don't like (criticism of the administration, support for Palestine, etc.) They usually tell you to unlock your phone and rely on your compliance. If you are a US Citizen, you do not have to unlock your phone or comply. If you are not a citizen, you risk being sent back to your country of origin if you do not comply and unlock your phone.

- [ ] **Know your rights when crossing the border**

  Your rights depend on your immigration status

Disclaimer: This is just information and not legal advice. Consult a lawyer for advice on your situation.

WHAT ARE YOUR RIGHTS WHEN CROSSING THE BORDER

We have summarized some information below, but we strongly recommend you read these articles to familiarize yourself with the nuances.

Read the following articles to learn your rights:

- Know Your Rights travel guide from stop AAPI Hate
- Is it safe to travel with your phone right now? from The Verge
- Can border agents search your electronic devices? It's complicated from the ACLU

> **Border police CAN search any electronic device** at airports/borders without a warrant, regardless of your status. Your rights to decline unlocking your phone depend on your immigration status.

US Citizens:

- **Cannot be denied entry** to the US
- **Must answer:** Identity and citizenship questions only
- **Can refuse:** Device searches and other questions (but expect delays). Device may be confiscated
- **Right to:** Legal representation at the border

Green Card Holders:

- **Cannot be denied entry** (without immigration judge hearing)
- **Must answer**: Identity and permanent residency questions
- **Can refuse**: Other questions and device searches (but you may face delays or deportation proceedings)
- **Don't surrender**: Your green card, even if pressured

Visa Holders:

- **Can be denied entry** for refusing searches or questions
- **Must answer**: All border police questions about travel, background, and purpose if you want to enter.
- **Device searches**: Refusal may result in visa revocation and deportation

If you're detained and questioned:

- **Never lie** - even small misrepresentations can lead to criminal charges
- **Stay calm** and tell the truth
- **Document everything** - officer names, badge numbers, questions asked
- **One phone call** may be allowed to notify someone.
- **Get a receipt:** If your device is not returned, get a receipt so you can attempt to track it down later.

Know the trade offs of not answering questions:

- While we would generally always suggest that you don't talk to cops, the situation at the border is more complicated. Citizens and non-citizens alike have fewer rights at the border.
- If you're a US citizen, you can refuse to answer questions (besides the basics listed above), but it may result in long questioning and your device not being returned to you.
- If you're a green card holder or visa holder, the risks are higher. Read the articles linked above to get a sense of your rights.

Keep your phone (and laptop) updated to the latest operating system version

Protects you from hackers, spyware, and the phone hacking tools the cops use.

DO: Install updates as soon as you're prompted

DO NOT: Keep pushing the "update later" button

Every time a new operating system update comes out, it is fixing security holes. Each update you haven't installed represents a longer list of ways the cops can hack into your device. Think of it as a big building with more and more doors left unlocked.

If your operating system is not up-to-date, many of the other recommendations in this guide will not protect your data.

Start with your phone. If you're doing something higher risk, make sure to update all your devices.

HOW TO RUN UPDATES

Because security updates are so important, **we designed a tool to walk you through the process**.

Check your phone and computer updates →

HOW TO RUN UPDATES MANUALLY

If you prefer to run updates manually, here is how to do it for each device:

Click to show the manual steps

Important Fully power off your phone & laptop before you approach security checkpoints

Fun fact: Your data is most secure when your phone/laptop is shut down before it's been unlocked the first time.

Almost all phones (and some laptops) are encrypted by default. When cops seize a device they will attempt to bypass the encryption. They'll have the hardest time breaking into a device that has been fully powered down (and has the latest operating system updates). If the passcode/password has been entered even once since booting up, extracting its data becomes a lot easier for them.

Encryption means that the data is scrambled and unreadable by anyone without the passcode or password.

Don't just put the device to sleep: A device with a blank screen might just be sleeping.

HOW TO FULLY POWER DOWN YOUR DEVICE

IPHONE

Press and hold **power** and **volume down** buttons → **Slide to power off**

ANDROID

Press and hold the **power button** → **Power off**

Laptop:

- Select **Shut down** from your system menu.
- In an emergency, almost all laptops can be forced to power down by pressing and holding the power button for 5-10 seconds

Power off your device: A fully powered down device is much more secure than one that is simply screen-locked.

Biometrics bonus: powering down *effectively disables biometrics* while crossing a checkpoint, since biometrics can't be used the first time after you power up your device (except those that use Windows Hello, so disable this for travel).

Set your phone passcode to 8 to 10 random digits

It takes years for cops to crack an 8-digit random passcode. They can probably guess your current passcode in less than 5 minutes with automated tools.

DO: Use a random passcode generator to create an 8 to 10-digit code

DO NOT: Use any passcode you thought of yourself (dates, patterns on the keyboard, etc.). Do not use 6-digit passcodes if possible.

HOW TO CHANGE YOUR PASSCODE

1. Generate a random 8 to 10-digit passcode using this random passcode generator. (Don't make one up yourself—humans are bad at choosing randomly!)
2. Change your passcode:

   IPHONE

   Settings → **Face ID & Passcode** → **Change Passcode** → **Passcode Options** → **Custom Numeric Code**

   ANDROID

   Settings → **Security** → **Screen Lock** → Enter Current Lock → **PIN/Password** → Enter a Passcode
3. **Practice the new passcode** at least 10 times in a row right now so you are more likely to remember it. (Disabling biometrics will force a passcode request every time you lock the phone.)
4. Write your new passcode on paper and keep it somewhere safe at home until you've memorized it. Then destroy it after 2–3 weeks. Setting a reminder on your phone can help.

How long does it take to crack a passcode?

TYPE	TIME IT TAKES TO CRACK (AVERAGE)	EXAMPLE
6-digit *easy-to-guess* pattern	**Less than 24 hours** to crack	*333666 (common pattern)* or *110585 (date pattern for Nov 5, 1982)*
6-digit *random* code	**200 days** to crack	*238253*
8-digit *random* code	**40+ years** to crack	*34780026*

Note: These times only apply to phones. Computers can be cracked much more quickly, and need much stronger passwords.

Sources: The estimates in the table above assume real-world observed attempts/second from police forensic hacking tools. If you need more security, use a 10-digit passcode, which will protect you even under the highest-possible cracking scenarios. See the sources linked in the passcode FAQ here.

Enable encryption on your laptop

Ensure your laptop is encrypted and secured with a sufficiently strong password.

If you have a strong password, disable face/fingerprint unlock, and enable disk encryption, your laptop and other devices will be very hard to access. **Encryption** is an essential part of these defenses. Without it, your password and other steps are basically meaningless if the state seizes your device.

HOW TO ENABLE ENCRYPTION ON YOUR LAPTOP (AND BACKUPS)

Encryption may need to be enabled on your laptop:

MACOS

System Settings → **Privacy & Security** [scroll to bottom] → **FileVault** → Click **Turn on...**

Save the **Recovery Key** in your password manager or somewhere secure. For maximum security, do not enable recovery using iCloud (but you will be required to remember your password and never lose it!)

WINDOWS

Settings → **Privacy & Security** → **Device encryption** → **Enable**

Also, make sure you have encryption turned on for your **external hard drives** and any backups you create.

Phone encryption: iPhones and modern Android phones are already encrypted by default.

Print a paper boarding pass and travel documents

So you can keep your phone fully powered off through security and customs.

DO: Power your phone down and use a paper boarding pass

DO NOT: Use your phone as your boarding pass

HOW TO PRINT YOUR TRAVEL DOCUMENTS

1. Boarding passes can usually be printed at the airport
2. For other travel documents like visitor or work visas or customs declarations, plan well in advance to ensure you can use paper, since some countries make traveling using an app the only convenient option.

Opt out of facial recognition at the airport (and wear a mask)

This helps make it harder for the government to develop a profile on you

DO: Say "I want to opt out of facial recognition" before you hand them your ID

In the United States, citizens have the right to opt out of facial recognition when passing through security (TSA). As of January 2026, non-citizens are now required to comply with facial recognition when entering and leaving the US.

TSA claims to delete photos within 24 hours in most cases. But we have seen many instances in the past where other facial recognition systems have experienced massive data breaches and that could happen here. You gain nothing from allowing the government to scan your face beyond your mandatory ID/passport photo.

YK Hong has an Instagram reel showing how to opt out and the reasons why it matters. We recommend their content on biometric theft.

HOW TO OPT OUT OF FACIAL RECOGNITION AT THE AIRPORT

You can and should opt out of facial recognition every time it is offered:

- Security screening (TSA, etc)
- The gate where you're boarding (some airlines are using facial recognition at the gate)
- Immigration and passport control (they have a camera to take your picture, but you can opt out).

It's easy to opt out:

1. Simply say **"I want to opt out of facial recognition."**
2. **Do not hand your ID over or put it in the scanner machine until the agent acknowledges your request.** Otherwise you may be locked into the facial recognition process.
3. **Wear a mask** for further protection when going through the airport. If you're wearing a mask, you will need to take it down so the TSA agent can make sure your face matches the photo on your ID.
4. If you're ever not sure what to do, just ask an agent nearby: "I'd like to opt-out of facial recognition, where do I go to do that?" They will often bring you to a separate line for manual screening (which sometimes gets you through faster!)

Enhanced protections

MEDIUM-THREAT This section might be for you if you are outspoken about immigration, Palestine, or other issues the government is targeting.

Note - Deleting data doesn't mean it's gone: This section suggests deleting apps and data. However, governments can use forensic tools to access data after it has been deleted. So the guidance below offers reliable protection only against an adversary manually searching through your device, which is the most common situation at the US border.

If you're at higher risk and think the cops might invest more resources to access the data on your phone/laptop, make sure to follow steps in the High-profile protection section below in addition to what's here.

- [ ] **Uninstall apps with sensitive data (email, docs, social media, etc) on phone and laptop**
  Remove anything you don't want to be easily searchable by the cops.

The less you have on your device, the better.

WHICH APPS TO UNINSTALL

Consider uninstalling the following apps (on phone and laptop) if they have any sensitive data in them:

- Email & Calendar apps (if you're using your phone's built-in apps you might need to sign out from your phone's **Settings** → **Accounts**)
- Docs & notes (Google Docs, Evernote, etc.)
- Other communication apps (Slack, WhatsApp, etc.)
- Google Maps (or at minimum disable Location History)
- Social Media apps

Tip: Hide the app: You can also move an app to a hidden folder. Instructions: iPhone and Android. This will only provide a slight advantage since most cops would know to look in this folder. Deleting is much more secure.

You may also want to **delete specific content** from apps that you leave installed:

- Notes in the built-in Notes app on iOS
- Individual text message threads
- Move sensitive photos to a Hidden Album (or alternately, back them up somewhere and remove them entirely from your device)

> **Empty the trash:** If you've deleted photos, notes, emails, or documents, there is often a "trash" or "recently deleted" folder where they are stored for 30 days. Make sure you go there and manually delete them immediately.

Backup Signal messages and delete the Signal app before entering a risky situation

Signal messages are often sensitive and something we want to protect from government surveillance.

The Signal backup feature is a great way to ensure your messages stay safe when you're headed into a situation where your phone might be confiscated or searched.

Backup Signal data and Delete Signal

HOW TO BACKUP SIGNAL DATA AND DELETE SIGNAL

1. **Enable Signal backups**: Open Signal → Tap your profile picture → **Settings** → **Backups** → **Enable Backups**
2. **Save your recovery key**: Save a copy of your recovery key in a secure location. We recommend using a password manager like 1Password.
   - If you want to be as safe as possible, you can send the recovery key to a trusted friend or family member who can read it back to you when you restore the backup later (so it's not stored digitally anywhere).
3. **Confirm your recovery key**: Signal will prompt you to confirm your recovery key to prove that you've saved it.
4. **Select your plan**: The "free" plan is enough for most folks. If you need more than the last 45 days worth of media (photos/videos/attachments), you can upgrade to the paid plan.
5. Then click **Back Up Now** to start the backup process.
6. **Delete Signal**: Finally, Delete the Signal app from your phone so the data is harder to access if your device is confiscated.

Keep the Recovery Key safe. If someone gets this key, they can read all of your Signal messages.

Laptop as well: If you are bringing your laptop and have Signal desktop installed, you'll also want to delete the Signal desktop app as well.

Data deletion isn't always complete: Deleting Signal does delete all the data associated. But if the state is willing to go to great lengths, there are ways they can sometimes still recover deleted data on a device. If you are in an extermely high-risk group, consider using a secondary phone that has minimal data on it instead of deleting Signal on your primary phone.

Restoring Signal data

Once you are ready to restore your Signal data, you can do so by following these steps:

HOW TO RESTORE SIGNAL DATA

1. Reinstall the Signal app on your phone.
2. Follow the steps to confirm your phone number.
3. When prompted, select **Restore from Backup** to restore your Signal data.
4. Enter your Recovery Key when prompted.

Uninstall your password manager (remember to back up your login credentials!)

Make sure to uninstall from your phone and your laptop.

If you don't use a password manager: Remove whatever method you use to store your passwords (like a notes doc or spreadsheet) - but make sure it's backed up elsewhere!!

Tip: If you use 1Password, just use travel mode for all your vaults except those essential for travel. Skip the instructions below.

HOW TO SAFELY REMOVE YOUR PASSWORD MANAGER

1. You must make **absolutely sure** you have memorized (or written down) your master password if you're uninstalling the app from all your devices. If you use 1Password, make sure to also write down your "Secret Key" and store it somewhere safe. You can travel with this information if you do not think your possessions will be searched.
2. Don't delete your Two-Factor Authentication (2FA) codes if you use an app on your phone for that. Those are hard to restore and not useful unless someone also has your password.

If you need passwords while traveling:

- Write your master password down on paper (and 1Password secret key if applicable). Conceal the passphrase innocuously (in a paper journal or dayplanner). Log back in after crossing the border. Burn this paper as soon as you're done with it.
- Alternatively, keep your passphrase (or part of it) with a trusted human who can share it with you on a secure channel (like Signal) from a safe location.

Hide or deactivate social media accounts

Helps protect you if they lookup your social media accounts online (without needing your device)

Unless you're intentionally trying to maintain a widely public social media presence, it's a good idea to lock down your accounts at least temporarily. (Consider doing it long-term for more privacy and security. Or just deleting the accounts outright if you can manage it.)

Visa applicants: If you are applying for a non-student visa, make sure you hide your social media before you apply. We know from the case of an Australian journalist that waiting until the week before you fly might mean they have already looked you up online.

Student visa applicants: In June 2025, the State Department started requiring all student visa applicants to make their social media profiles public. If this applies to you, you may want to actually delete old posts using a tool like Block Party.

HOW TO HIDE OR DEACTIVATE SOCIAL MEDIA ACCOUNTS

Instructions:

1. **X / Twitter:** make it private or deactivate it
2. **LinkedIn:** make it private or deactivate it
3. **Instagram:** make it private or deactivate it
4. **Facebook:** make it private or deactivate it
5. **TikTok:** make it private or deactivate it
6. Consider hiding other public posts like blog posts, YouTube videos.

Consider using Block Party to assist with this process; Cyd.social can also help you make a local, private backup first!

While hiding your posts against the government might help you get into the US safer, we still need to keep speaking out publicly through posts, protests, and boycotts, because staying quiet might protect us individually but helps the authoritarian system we're fighting against.

You are not obligated to provide your social media handles to CBP (Customs & Border Patrol) or to the TSA. You can say that you are not comfortable answering or that you do not see the relevance of the question to your travel. Do not volunteer additional information for any question.

Log out of websites that have sensitive information (phone and computer)

If you're not signed in, you have more legal standing to not reveal your password

WHICH WEBSITES TO LOG OUT

Remember to log out on both your phone ***and*** your laptop.

Websites to log out of:

- Email and calendar (work and personal)
- Docs (Google Drive, etc)
- Social media
- Discussion forums (Reddit, etc)

And anything else you wouldn't want the cops looking at.

Leave Signal groups that might put others at risk

This helps protect your network if your phone is confiscated.

If your phone is confiscated by law enforcement, one of the biggest risks is exposing your entire network. Even if people aren't using their real name on their Signal account, there is still a unique ID behind every Signal username. And the cops can use this to correlate someone's identity across many seized devices.

You need to both leave AND delete the group:

- If you only leave the group, old messages stay on your phone as well as the history of who was in the group.
- If you only delete the group, new messages will still come through and the thread re-appears.

HOW TO LEAVE AND DELETE A SIGNAL GROUP

1. **Make a plan to re-join afterwards:** When headed into a situation with possible arrest, make a list on paper at home or somewhere safe of all the groups and who you need to message who can re-add you after the action or border-crossing is complete.
2. **To leave the group:** Signal → [Group] → Tap the group icon at the top → **Leave group**
   - If you're the only admin, you have to either remove all members or assign another admin.
3. **To delete the group from your phone:** Signal → Main screen → Swipe left on the thread → **Delete**
   - This won't delete it for anyone else.

Security hygiene tips:

- Set a recurring reminder to clean up your Signal thread every 3 months.
- Make sure you take note of which groups you are leaving and who you can ask to re-add you after the action.

Note: If you find this process very annoying and cumbersome (because it is!), that's another good reason to use a secondary phone for actions. That phone would only ever be in the one or two groups needed to pull off the action that day.

Install a trusted VPN app with ad-blocking to make it harder for cops to do warrantless surveillance

A VPN makes it harder for websites to track you and prevents your internet provider from logging your traffic.

DO: Install a trusted VPN app on your device(s) and keep it on. We recommend IVPN ($6/mo).

DO NOT: Use a random VPN you find online. Nord VPN, Surfshark, ExpressVPN, etc, are popular but not as trustworthy.

Anytime you connect to the internet (phone or computer), your internet provider is revealing your approximate location to every site/app you use.

We know that law enforcement agencies are using tools to track your location using data gathered from apps you have and ads you see. Using a VPN with ad-blocking features enabled makes it much harder for them to track you. Also, a vetted VPN won't track your browsing; police can get a subpoena for your internet traffic that gets tracked by your internet provider.

A VPN helps mask your location and makes you slightly harder to identify.

A VPN with ad-blocking enabled on your phone can help prevent warrantless location tracking (through ad networks).

Check out our dedicated VPN page for more info on when a VPN is actually useful and when it is not.

A VPN doesn't make you fully anonymous. For sensitive browsing requiring higher anonymity, consider Tor Browser as a second browser alongside your everyday one.

Options: These are the VPNs we recommend for most activists (see our full list of vetted VPNs):

- **IVPN (top recommendation)**: Easy to use and renews automatically.
- **Proton VPN** has a solid free plan, but it is only for 1 device. To get ad-blocking, you need a paid plan. (If you use Proton, see our guide to using Proton safely.)

HOW TO SET UP IVPN

1. **Generate your account:** Go to IVPN and click Generate IVPN Account ($6/mo or $60/yr). Under **Standard Plan** click **Select** (choose the **Pro Plan** if you have more than 2 devices).
2. **Write down your Account ID:** Save it somewhere safe like your password manager. There is no "forgot password" option, so if you lose it, no one can recover it for you.
3. **Pay:** Select monthly or yearly, check the **Automatic renewal** box, enter your payment details, and click **Make Payment**.
    - Instead of a credit card, you can also order a voucher card for IVPN so that your identity is even more protected.
4. **Install the desktop app** (Mac, Windows) and sign in with your Account ID.
5. **Enable autoconnect:** Find IVPN in your toolbar → **Show IVPN** → ⚙️ **Gear Icon** → **Settings** → **General** and enable **Launch at login**, **Autoconnect on launch**, and **Allow background daemon to manage autoconnect**.
6. **Enable ad-blocking:** Turn on **AntiTracker** in the main IVPN app screen to block ads (which can help you keep your location private, especially on your phone).
7. **Install the mobile app** (iPhone, Android) and sign in with the same Account ID, then turn on the same settings listed above. (Autoconnect is not a setting on iPhones because it is on by default.)

We recommend keeping your VPN on at all times unless you're having trouble connecting to a site (see our list of downsides to using a VPN).

Why we no longer recommend Mullvad: Mullvad used to be the #1 most-recommended VPN by activists and at-risk populations. Their VPN technology is still the best out there, but one of their co-founders recently ruined their stellar reputation by donating hundreds of thousands of dollars to a far-right political party in Sweden. So we can't recommend them anymore.

High-profile protections

HIGH-THREAT **This section is for you if:**

- → You are not a natural-born US Citizen.
- → You are doing activism, community organizing, or other work against the administration that puts you in a **position of power** or **public prominence**.
- → You are a public figure (artist, scientist, human rights lawyer) that has spoken out very publicly against the administration.
- → You have any other reason to think you might be a more of a target than most folks crossing the border.

This section assumes that border agents might go further and attempt to hack your device using forensic extraction tools. The best approach in this case is to bring a secondary device (sometimes called a "burner phone" or "travel laptop"). Because you can be denied entry or have devices seized indefinitely, your goal should be to travel with devices that you would be able to unlock and display to a border agent. Avoid if at all possible the device being taken from your hands or out of your sight.

☐ Prepare a secondary phone (and keep very little information on it)

If you bring a phone with very little data on it, it won't matter much if they get access to it.

HOW TO SET UP A SECONDARY PHONE

Take the Secondary Phone Checklist steps, but with the following changes:

1. Instead of getting a SIM with a US phone number, search online for prepaid SIMs you can buy in advance for the country you are going to.

   Or alternately, just use the phone on Wifi without a SIM or phone number until you arrive in the country, then buy a SIM card near the airport when you arrive. For eSIM-enabled phones, alosim.com can be a convenient option.

   - Only do this when departing the US. When re-entering the US, make sure before you pass through customs you will be able to access either airport WiFi or an active SIM to communicate with your emergency contacts.
2. As stated in the Secondary Phone Checklist, store only essential, absolute minimum information on the device.
3. If you set up Signal with a new phone number (from your new SIM card), make sure you add only your most essential contacts.
4. Do NOT sign into any websites with sensitive information: email, social media, etc.

Alternate approach: If you can't access a secondary phone, you can also backup your entire phone to your computer (iPhone, Android) NOT the cloud. Then you can factory reset your phone and use it while on your trip. When you return, you can then do another factory reset and restore from the backup. If you take this approach, ensure you have a backup of your backup in a secondary location. Backing up an iPhone to the cloud with Advanced Data Protection could be considered safe.

☐ Prepare a secondary laptop (if applicable)

If you can manage without a laptop, that's safer. If you need a laptop on your trip, we suggest getting a secondary device and keeping very little data on it.

SETTING UP A SECONDARY LAPTOP

1. Try to find an old one from a friend that you can use or buy a cheap one online.
2. Factory reset the device (Mac, Windows)
3. Set up the device without signing into your typical Apple/Microsoft account (which risks syncing a lot of data to the machine).
4. Install only apps that have data on it that you'd be okay displaying to a border agent.
5. Do NOT download or install secure apps like Signal, your password manager, or apps with a lot of information like Google Drive (for desktop) or Gmail.
6. Do NOT sign into any websites with sensitive information: email, social media, etc.

After you cross the border, if you install additional apps, make sure you remove them again before you re-cross the border.

If your only concern is crossing the US border (traveling from the US to a low-risk destination) you could plan to use your usual laptop for travel, then factory reset the laptop before returning to the US. It would serve the same purpose as a "secondary laptop." To do this, start at step 2 above.

If you'll be using your everyday laptop as a travel laptop, **fully back up your laptop** before you leave, and plan to **sync all travel work you want to keep** to a secure cloud location (Proton Drive is best for secure items, but Google Drive and others can work if it's not highly sensitive) before factory resetting. Ensure the laptop's disk is encrypted first.

Generate a random passphrase for your laptop (if you're bringing it)

The encryption on your devices is only as strong as your passphrase. If you think of a passphrase yourself, it is likely much easier to crack than one that is randomly generated.

HOW TO SET A RANDOMLY-GENERATED LAPTOP PASSWORD

1. Generate a computer-generated, random passphrase using a site like StrongPhrase.net
2. Change your password on your device:

   MACOS

   System Settings → **Users & Groups** → Click the circle "i" icon ℹ️ next to your account → Click **Change...**

   Then use the passphrase you generated above.

   WINDOWS

   Settings → **Accounts** → **Sign-in options** → **Password** → **Change** → Enter current password

   Then use the passphrase you generated above.

Make a safety plan with 2+ emergency contacts

Make sure someone can help you if you're detained at the border.

HOW TO MAKE A BORDER CROSSING SAFETY PLAN

1. **Contacts:** Ask 2-3 people to act as your emergency contacts
2. **Contact information:** Make sure you memorize their phone numbers. Do this a week or more before you depart if possible.
3. **Group:** Put them in contact with one another so they can coordinate if they need to support you.
4. **Arrival/departure information:** Let them know your departure/arrival times and your flight number so they can track your flight online in case there are delays.
5. **Legal information:** Also, tell them your government ID number, passport number, full legal name, and date of birth. These can be helpful if you are detained.
6. **Reception:** Make sure you will either have WiFi at the airport or a functioning SIM card.
7. **Legal support:** Tell them how they should go about finding legal support for you if you are detained. Either identify a lawyer who you already have a relationship with or tell them how to find lawyers who support activists (check out the ACLU and the NLG). If you're at especially high risk, then make sure you've made contact with a lawyer in advance and let them know who your emergency contacts are.
8. **Check in plan:** Let them know **when** and **how** you will contact them before and after you go through US customs and immigration at the border. Ensure they have **clear steps to follow** if you do not check in.

For example:

> "I will message you on Signal after my flight lands and before I go through customs. I'll message you from 555-123-4567. I started a Signal group for us already. If it's been more than 1 hour since you last heard from me, notify my legal support. If my lawyer agrees it is strategic to do so, put out a public call for support. Please water my plants and let my work know I'm delayed in transit."

Write down contact information for anyone you need to be in touch with

HOW TO MANUALLY TRACK YOUR CONTACTS

1. Instead of syncing all your contacts from your main phone, write down on paper (or digitally) the most important contacts that you will need on your trip. Include their phone number and email address.
2. Make sure to let them know what phone number and/or email address you will be contacting them from, and consider a pre-arranged check-in question/answer so they can verify that it is you and not someone impersonating you.

Fully disable face/fingerprint unlock (biometrics)

Protects you if the cops try to force you to unlock your phone.

Cops can try to force you to unlock your phone with your face/fingerprint (though this is supposed to require a warrant, but that doesn't mean that always happens).

You have stronger legal standing with a passcode than with biometric unlock.

HOW TO DISABLE FACE/FINGERPRINT UNLOCK

IPHONE

Settings → **Face ID & Passcode** → Disable **Use Face ID for iPhone Unlock**

(You can leave the rest enabled.)

ANDROID

Settings → **Lock Screen** (or **Security**) → **Biometrics and Security** → **Disable both Face Recognition and Fingerprint Unlock** for unlocking your phone

Caveat: Face/fingerprint unlock can make it easier to use a strong passcode without typing it every time. If you feel you have to choose between a long passcode and disabling biometrics, we recommend a longer passcode.

iPhone locking tip: To force your passcode on the next unlock, either press the side button 5 times rapidly, or hold the side button and either volume button for a few seconds.

Test first: depending on your settings, these gestures may also start a countdown to call emergency services. You can change that.

Note: Doing this does not protect your data from phone hacking tools that cops use. The only way to do that is to fully power off your device.

Android locking tip: On most Android phones, you can temporarily disable face/fingerprint unlock by holding down the power button and tapping "Lockdown" on the menu that appears.

iPhone camera tip: You can take photos without unlocking your phone by **swiping left** on your home screen. (In case you get arrested while filming.)

Android camera tip: For most Android phones, you can open the camera without unlocking your phone by double-pressing the power button.

- [ ] **Follow all the steps in the first two sections of this guide**

All the steps in the Baseline Security Approach and Medium Security Approach sections above still apply even if you're using secondary devices.

Learn more

- Is it safe to travel with your phone right now? - The Verge (2025)
- Preparing devices for travel through a US border - Freedom of the Press Foundation (2025)
- Digital Privacy at the U.S. Border - Electronic Frontier Foundation (2017)
- We strongly suggest you opt out of facial recognition at the airport (US Citizens only). Check out this printable card to know your rights. Follow YK Hong (Instagram, blog) for more.

Frequently asked questions

Can CBP search my phone at the US border?

Do I have to unlock my phone for border agents?

Should I use a burner phone to cross the border?

Is airplane mode enough to hide my location?

What about social media before I apply for a visa?

Reports of device searches at borders

These stories can be frightening to read, but they can also help us understand the specific threats that people crossing the border are facing. Since immigration/citizenship status makes a difference in this situation, we've separated the stories:

Non-citizens:

- 2025 June - Australian independent journalist deported for his reporting on the Columbia Palestine solidarity encampments. Takeaways: lock down your social media and public before you apply for a visa, not before your flight.
- 2025 March - French researcher denied entry for being critical of Trump administration

Citizens:

- 2025 April - Black, Muslim, pro-Palestine activist detained and had devices confiscated when re-entering the US
- 2025 April - Civil rights lawyer detained and phone seized because they represent a pro-Palestine protester

Keep learning with these related guides

Secondary phone
Set up an extra phone for activism and protests.

Security essentials
Core security practices every activist should follow.

Signal security
Secure your Signal messaging app for safer communications.