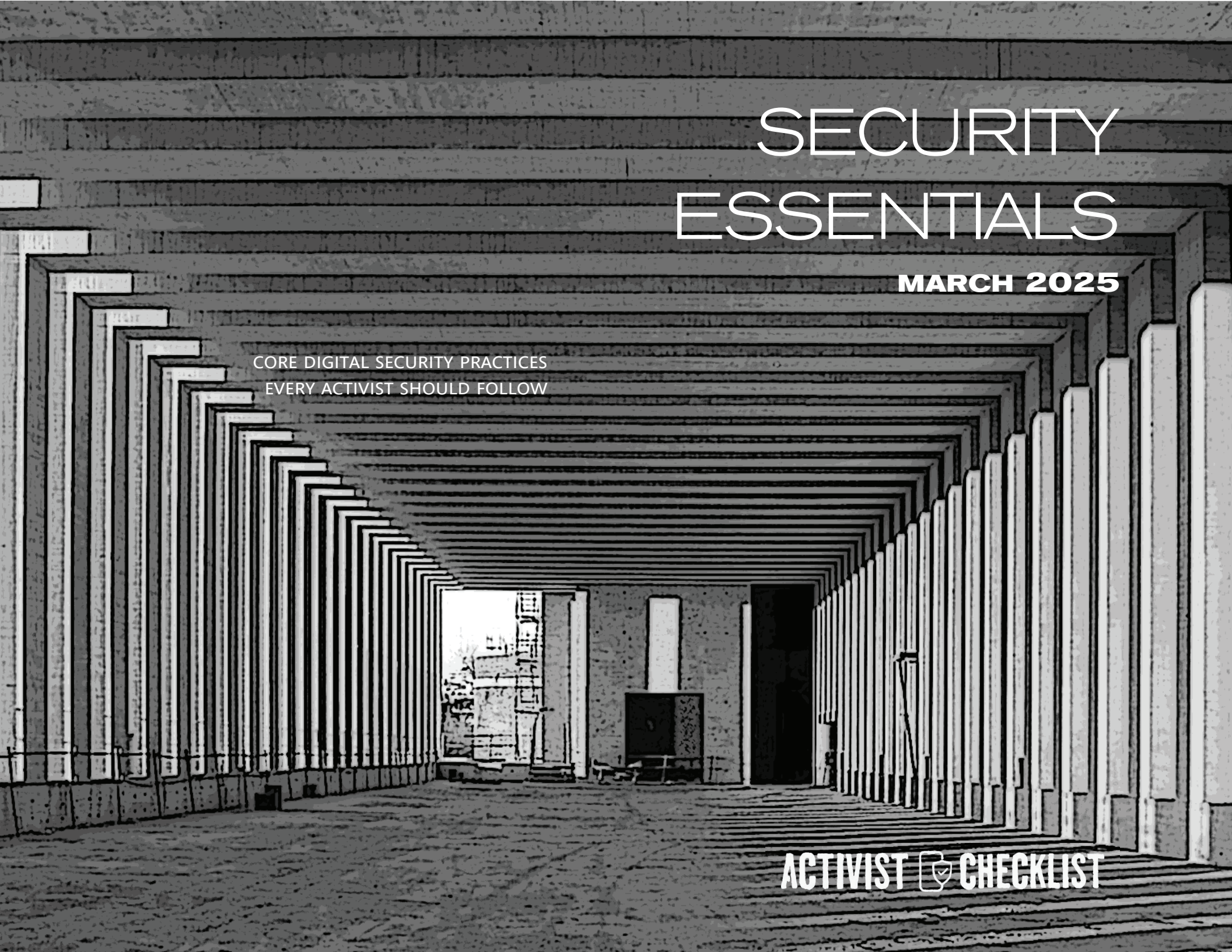

SECURITY ESSENTIALS

MARCH 2025

CORE DIGITAL SECURITY PRACTICES
EVERY ACTIVIST SHOULD FOLLOW

ACTIVIST CHECKLIST

SIMPLE GUIDES TO KEEP US MORE SAFE

We built this because digital security shouldn't be overwhelming. We take a harm reduction approach: start where you are and do what you can.

Find more guides like this on *activistchecklist.org*

CONTENTS

BASELINE SECURITY

Every click, message, and location ping creates a digital trail that can be used against activists and organizers. Law enforcement regularly demands data from tech companies to identify and surveil people working for social change.

This guide helps you minimize your digital trail. These steps won't make you invisible, but they'll make it substantially harder for authorities to:

- Track your location and movement patterns
- Monitor your communications and political discussions
- Map your relationships and networks
- Build profiles of your activities and associations

Use Signal for texts and calls, especially your activism and political conversations

Normal calls and texts are insecure and can be turned over to the cops.

DO: Use Signal

DO NOT: Use WhatsApp, FB Messenger, Telegram, regular texts, etc.

HOW TO SET UP SIGNAL

1. Install **Signal**[1] on your phone
2. You can now message your existing contacts using their phone number (they must have Signal installed as well). If you're messaging someone new who you don't yet have trust with, you should exchange usernames instead of phone numbers when possible.
3. To start a new message: Press the "Create" icon in the top right of Signal, then type in either the person's phone number or username
4. Follow the Signal Checklist to make sure you have the most security and privacy

1 https://signal.org/

Avoid using "Sign in with [Google, Facebook, etc]"

Every time you use "Sign in with Google" (or similar options) you're letting Google track which services you use and connect them to your real identity. Creating separate accounts with unique passwords (using your password manager) makes it harder for corporations and authorities to build a complete picture of your online activities.

DO: Create an actual account with your email address when signing up on a new site

DO NOT: Use "Sign in with [Google, Facebook, etc]"

Follow our phone security checklist

HOW TO SECURE YOUR PHONE

For added privacy and security on your phone, follow as many of the steps in our *Prepare for a Protest* guide as you are able to in your daily life, even if you're not at a protest/action.

When to use signal

Some examples of when you would especially want to use Signal

- Discussing a protest/action that is not public
- Organizing a protest/action that is public, but the organizers want to protect their privacy
- Criticizing government and power holders

Keep speaking out publicly! We encourage Signal (or just in-person conversations with no tech around) to have secure channels where we can speak more freely to get organized for public engagement. That said, we should encourage one another to continue to speak out publicly about our criticisms of power holders. As Timothy Snyder says, do not obey in advance.

Use privacy-focused browser for everyday browsing (instead of Chrome).

Minimize tracking, so there's less of a digital trail.

DO: Use Brave Browser (easiest) or Firefox (more setup required)

DO NOT: Use Google Chrome, Microsoft Edge, etc.

- We recommend **Brave**[2] because it offers the most privacy without any additional configuration, which is our goal on this site.
- **Firefox**[3] can offer even more privacy if you take the time install the right plugins and configure it properly.[4]
- Use **Tor Browser**[5] for highly sensitive browsing that is truly anonymous

HOW TO SET UP BRAVE BROWSER

Brave is a privacy-focused browser that allows you to install Google Chrome extensions.

1. **Install Brave** on your computer (or phone).

2 https://brave.com/
3 https://www.mozilla.org/en-US/firefox/
4 https://www.privacyguides.org/en/desktop-browsers/#firefox
5 https://activistchecklist.org/research

How long does it take to crack a passcode?

TYPE	EXAMPLE	TIME IT TAKES TO CRACK
Easy-to-guess pattern	*333666 (common pattern) 110585 (date pattern for Nov 5, 1982)*	**Less than 5 minutes** to crack
6-digit *random* code	*238253*	**12-24 hours** to crack
10-digit *random* code	*3478002641*	**6+ years** to crack
3 random "diceware" words (generator)	*horse battery staple*	**200+ years** to crack

Note: These times only apply to phones (with an up-to-date operating systems). Computers can be cracked much more quickly. and need much stronger passwords.

Set your passcode to 10 or more random digits

It takes 6+ years for cops to crack a 10-digit random passcode. They can probably guess your current passcode in less than 5 minutes.

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

DO NOT: Use dates, easy-to-guess patterns, or 6-digit passcodes

HOW TO CHANGE YOUR PASSCODE

1. Generate a random 10-digit passcode.[1] (Don't make one up yourself—humans are bad at choosing randomly.)
2. Change your passcode:
3. On iPhone: Settings > Face ID & Passcode > Change Passcode > Passcode Options > Custom Numeric Code
4. On Android: Settings > Security > Screen Lock > Enter Current Lock > PIN/Password > Choose 10-digit Passcode
5. Write your new passcode on paper and keep it somewhere safe until you've memorized it.

1 https://strongphrase.net/#/passcode

2. Follow the steps after you launch to import your configuration from Chrome or another browser. (See warning below about how plugins make you more identifiable.)
3. **Configure privacy settings:** Go to Brave > Settings > Shields then select the following:

- Select **Aggressive** under "Trackers & ads blocking"
- Select **Strict** under "Upgrade connections to HTTPS"
- Uncheck everything under **Social media blocking**
- (Optional) Enable **Forget me when I close this site.** The site won't be able to store anything about you after your reset your browser.

This will make it harder for sites to track you across the internet. It's good for privacy, but you'll want to manually override this for specific sites. Visit the site > Click the Brave (lion) logo in the URL bar > Advanced controls > Disable "Forget me when I close this site"

Optional:

1. Disable the annoying new tab page: Brave > Settings > Get started > New Tab Page > Select "Blank page" from the dropdown
2. Disable toolbar items: Brave > Settings > Appearance > Toolbar > Disable all the toolbar buttons that you don't want (Brave Rewards, VPN, Wallet, Leo AI, etc)

Plugins warning: Every plugin you install makes your browser stand out from "the crowd" and makes you more identifiable, reducing the effectiveness of the privacy features built-in to Brave.

Bonus Brave configuration tips:

- Install Privacy Badger for some added protection.
- You can install the iPhone or Android Brave app as well.

Install a trusted VPN (IVPN or Mullvad)

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

DO: Install a trust VPN and keep it on. We recommend IVPN ($6/mo) or Mullvad VPN ($5/mo)

DO NOT: Use Google Chrome, Microsoft Edge, etc.

A VPN (Virtual Private Network) encrypts your internet traffic and masks your location. This means your Internet Service Provider can't see what sites you visit - they only see you connecting to a VPN. Websites you visit will see the VPN's location and IP address instead of yours. This makes it harder for authorities to build a record of your political activities.

A VPN does NOT make you fully anonymous online. If you need higher anonymity for highly sensitive web browsing, you'll want to look into using Tor Browser[6]. You can always use multiple browsers: one for everyday private browsing and one for tasks that require more anonymity.

6 https://activistchecklist.org/research

ENHANCED SECURITY

If you're taking higher risk actions or are more likely to be a target of government surveillance, follow these steps will help you add additional layers of protection

HOW TO USE PROTON MAIL

Creating a Proton Mail account

- Sign up for a free ProtonMail account
- Choose a random username that isn't connected to your identity or preferences
- When asked to verify if you are a human, choose the "CAPTCHA" option rather than the "email" option.
- When asked to set your phone number / email as a recovery method, choose **Maybe later.** (Note: This means you must save your password somewhere secure like a password manager.)

Sending emails securely

- Messages between Proton Mail users are automatically end-to-end encrypted.
- Messages to people using a different email provider will not be encrypted, but you can send a password-protected email.

Options: All of these are very trustworthy options.

- **IVPN (our top recommendation)**[7] is easier to use. Cheapest if you have 2 devices.
- **Mullvad VPN**[8] enhances privacy by not allowing recurring subscriptions, so they can't store payment info about you. But you have to remember to pay each cycle. It's also cheaper for 3+ devices.
- **Proton VPN**[9] has a solid free plan, but it is only for 1 device and we recommend See our note below about concerns about the Proton CEO and why we still offer Proton options.

HOW TO SET UP IVPN

1. Go to IVPN and click Generate IVPN Account ($6/month or $60/year)
2. Under "**Standard Plan**" click Select. You can do the Pro Plan if you have more than 2 devices.
3. Write down your **Account ID** somewhere safe, like where you store passwords. You cannot recover it with "forgot password." If lost, no one can help you recover it. Keep it somewhere secure (ex: password manager).
4. Select monthly/yearly and enter your credit card or payment details.
5. Instead of a credit card, you can also order a voucher card for IVPN or Mullvad so that you identity is even more protected. (Yes, we hate Amazon too, but that's the only place online you can buy these cards.)

---

7 https://www.ivpn.net/en/
8 https://mullvad.net/en/vpn
9 https://protonvpn.com/

6. Check the **Automatic renewal** box then click **Make Payment**.
7. Download the **IVPN app** for your computer: Mac, Windows
8. Follow the instructions to install the app.
9. Find the app in your toolbar > Show IVPN > Click the gear icon to **open settings** > General. Enable the following: Launch at login, Autoconnect on launch, and Allow background daemon to manage autoconnect
10. Install IVPN app on your phone: iPhone, Android
11. Follow the the same instructions to enter your Account ID and configure the same settings. (iPhones don't offer the "auto-connect" setting, but it does auto-connect by default).
12. We recommend keeping your VPN on at all times unless you're having trouble connecting to a site (see below).

Downsides to using a VPN

- You will encounter more CAPTCHAs on websites
- Some websites may block VPN access
- Some streaming services might not work

If you experience odd behavior on websites, always try turning off the VPN temporarily to see if it will load. (IVPN offers a "pause for 5 minutes" option, which helps you not have to have to remember to turn it back on later.)

Note: You must use a trusted VPN that doesn't keep logs of your internet traffic and will push back on government requests. We've vetted our top recommendations

What NOT to use email for (even encrypted):

- Truly sensitive or private communications (example: when planning a direct action)

Concerns about Proton CEO

Proton Mail's CEO recently praised a Trump appointee. After investigating this, we've decided to continue recommending certain Proton services. While concerning, we view this as an unfortunate misstep rather than a threat to user privacy or data security. We believe in recommending tools that balance strong security with usability - ones that people will actually adopt and use. We will keep an eye on it and change our recommendations if they make more concerning moves.

If you want to put in the work to use a different system, there are other options like Tuta and Mailbox.org.

Proton Mail is not end-to-end encrypted in most cases

Contrary to popular belief, Proton Mail does not end-to-end encrypt all of your emails. **If you send email to someone using a regular email service, your messages will not be end-to-end encrypted.** Only your emails to other Proton Mail users (or other people using an encrypted email service) are encrypted. That said, getting off Gmail still makes it harder for your emails to be accessed by the government through backdoors, etc.

Don’t use email for secure communications

Email wasn’t designed to be private or secure.

DO: Avoid using email for secure communications (but use Proton Mail if you need to)

DO NOT: Send unencrypted emails with sensitive information

Email wasn’t designed to be private or secure. For sensitive communications, use Signal instead.

Anonymity vs secure communications: It’s very hard to have truly secure email communication, but if you are looking to protect your message contents, then you can use a service like Proton Mail.

What to use Proton Mail for

- Creating accounts on websites, signing up for newsletters
- Public-facing communications that don’t need to be secure, but do need to be anonymous
- Organizing work that isn’t sensitive

Ditch Google Search and use a search engine like Brave Search instead

Your search history tells a lot about your interests and political leanings.

DO: Use a privacy-respecting search engine like Brave Search or DuckDuckGo.

DO NOT: Use Google Search, Bing, Yahoo, etc.

- **Brave Search**[10] tends to have better results and we trust them, but some folks don’t align with their business model
- **DuckDuckGo**[11] results aren’t as reliable but it has a slightly stronger privacy record.

HOW TO SET UP PRIVATE SEARCH

- **Brave Search**: If you’re using Brave browser, it’s the default. If you’re using another browser, you can follow these instructions.[12]
- **DuckDuckGo**: Follow these instructions to make DuckDuckGo your default search engine.[13]

10 https://search.brave.com/
11 https://duckduckgo.com/
12 https://search.brave.com/default
13 https://duckduckgo.com/duckduckgo-help-pages/change-default-search-engine/

Install the latest software updates for your laptop, phone, and apps

The latest updates for your computer, phone, and apps all contain security fixes that help keep your system safe from attackers.

DO: Run updates as soon as they are offered

DO NOT: Keep pressing the “update later” button

HOW TO RUN UPDATES

MODEL	STILL ELIGIBLE FOR SECURITY UPDATES?	OPERATING SYSTEM	APPS
iPhone	Check for iPhone models	Update operating system	Make sure you enable automatic updates (enabled by default).
Android	Check for Samsung models Check for Google Pixel models	Update operating system	Make sure you enable automatic updates (enabled by default).
Mac	Make sure your mac isn't on this “obselete“ list (ð > About This Mac)	Update operating system	• App Store apps: Make sure you enable automatic updates (on by default). • Other apps: Top Menu > [App Name] > Check for updates..
Windows	Try to update, then see if your version is supported here	Update operating system	• Microsoft Store apps: Make sure you enable automatic updates (on by default). • Other apps: Try Menu bar > Help > Check for Updates. Or look for “Updates” or “About” under settings.

Don’t click suspicious links in texts

High-profile activists and human rights advocates have been targeted with specific spyware that gets activated when you click a link to a website you don’t trust.[22]

22 https://theintercept.com/2021/07/27/pegasus-nso-spyware-security/

2. **Option 2: Ente Auth:** Install Ente Auth[21] (iPhone, Android)
    - Optional: You can create an account. Your data is end to end encrypted. Or you can not have an account, but you may lose your one time passwords if your phone is not backed up.

To set up two-factor authentication:

1. Go to Security/Privacy settings
2. Look for "2FA" or "two-factor authentication" or "multi-factor authentication"
3. If an "authenticator app" option is available, select that! (Remember to save the backup codes somewhere secure, like your password manager.)
4. If "text/SMS verification" is the only option, select that and follow the instructions.
5. Links to set up 2FA on common sites:
    - Google
    - Apple ID
    - Facebook
    - Twitter / X
    - Instagram
    - Or look up whether a website/service/app has 2FA on the 2FA Directory.

Note: When a service allows you to choose between an authenticator app and SMS text message verification codes, opting for the authenticator app is always best. It's possible for an attacker to intercept your SMS texts.

21 https://ente.io/auth/

Use Organic Maps or Apple Maps for navigation

While Google has recently started to make it harder for police to request location data, they have a terrible record on privacy and shouldn't be trusted.

DO: Use Apple Maps or Organic Maps for navigation

DO NOT: Use Google Maps

Apple Maps (iPhone only) goes to surprising lengths to protect your privacy.[14] Apple has a much better privacy track record than Google, but they are a big tech company so we should think of Apple Maps as a "harm reduction" choice that is good for every day use but not for sensitive organizing. We include Apple Maps as a recommendation here because there are some features (traffic, public transportation) don't exist in other apps.

HOW TO SET UP APPLE MAPS (IPHONE ONLY)

1. Apple Maps is installed by default (you can re-install it if you removed it).
2. Go to Settings > Privacy & Security > Location Services > System Services, then disable iPhone Analytics, Routing & Traffic, and Improve Maps.

14 https://youtu.be/alodEeY6YAM?t=137

Organic Maps (iPhone or Android) is a less user friendly than Apple Maps, but has much strong privacy. You can operate it entirely offline, which is especially helpful for activists. That said, it doesn't have live traffic data or public transit routes, which makes it hard to use as your main option. We wish there a better everyday option for Android phones.

HOW TO SET UP ORGANIC MAPS (IPHONE OR ANDROID)

1. Install Organic Maps[15]
2. Open the app once in your area and it will automatically prompt you to download the data for offline navigation

15 https://organicmaps.app/

Enable two-factor authentication

If someone steals your password, two-factor authentication keeps them from being able to get in unless they have your phone too.

DO: Enable two-factor authentication for important sites

DO NOT: Use only a password

After entering your password, you'll need to enter a code from your phone to prove it's really you. Think of it like having both a key and an alarm code to get into your house—someone needs both to get in.

Your email is the most important account to have two-factor authentication. If an attacker gets access to your email, they can reset all your other passwords.

HOW TO SET UP TWO-FACTOR-AUTHENTICATION

Install an authenticator app:

1. **Option 1: 1Password**: If you're using 1Password[20], it has an "authenticator" feature built-in (details here).

20 https://activistchecklist.org/essentials/#password-manager

3. **Import**: Import your existing passwords from your computer or browser
4. **Apps**: Install the browser extension and mobile app (iPhone, Android) to help you save and auto-fill passwords
5. **Change passwords**: If you had been re-using similar passwords, update your most important ones using the random password generator built-in to 1Password.

See 1Password's getting started guide[18] for a video of these steps.

Bonus: Here's a good introduction on how to get the most out of 1Password.[19]

Alternative options:

- Proton Pass: has a free option
- KeyPassXC: Open-source and allows you to store passwords only on your machine instead of the cloud, but the user interface is very clunky.

18 https://support.1password.com/explore/get-started/
19 https://www.nytimes.com/wirecutter/guides/how-to-use-1password/

Turn off location tracking for most apps

Apps with location access can create a detailed map of your movements, which can be accessed by law enforcement through legal demands or data brokers through purchase.

DO: Turn off location tracking for most apps

DO NOT: Let every app know where you are

HOW TO REVIEW LOCATION PERMISSIONS ON IPHONE

1. Go to Settings > Privacy & Security > Location Services
2. Review each app and set to one of these options:
   - **Never**: Best choice for most apps
   - **Ask Next Time Or When I Share**: Good for apps you rarely need location for
   - **While Using the App**: Only for essential navigation apps
   - **Always**: Almost no app should have this permission
3. Make sure to set the Photos app to "Never" so you don't risk revealing your location when sending photos.
4. Go to the app labeled System Services > Disable Significant Locations

HOW TO REVIEW LOCATION PERMISSIONS ON ANDROID

1. Go to Settings > Privacy > Permission manager > Location
2. Review each app and set to one of these options:
   - **Don't allow**: Best choice for most apps
   - **Ask every time**: Good for apps you rarely need location for
   - **Allow only while using the app**: Only for essential navigation apps
   - **Allow all the time**: Almost no app should have this permission

It is especially important to disable location tracking for your camera/photos app

These apps might genuinely need location while in use:

- Navigation (Apple Maps, Organic Maps)
- Ride-sharing (but only while actively using)

Some apps might need temporary permission:

- Food delivery apps only need location when you're actually ordering

Apps that definitely do NOT need location access:

- Photo apps
- Social media apps
- Games
- Most shopping apps
- Banking apps
- News apps
- Most productivity apps

Remember: Every app with location access is a potential privacy leak. When in doubt, disable location and only re-enable if you find you actually need it.

Use a password manager with strong passwords

When you use the same password on multiple sites and one site gets hacked, a hacker can gain access to many other accounts. If you use a weak password, the cops will have an easier time targeting you.

DO: We recommend 1Password ($3/month) or Bitwarden (free)

DO NOT: Use weak/identical/similar passwords. We don't recommend using LastPass.

Our main recommendations are:

- **1Password**[16]**:** Very user friendly. Slightly more secure. Costs $3/month
- **Bitwarden**[17]**:** Free. Still quite secure.

HOW TO SET UP 1PASSWORD

1. **Download**: Download and install 1Password ($3/month)
2. **Master password**: Create a strong, random "master password" using a passphrase generator. It should be memorable, but not a password you use anywhere else. Write your master password down on paper rather than storing it digitally. Set a reminder to destroy the paper in a few weeks once you have it memorized.

16 https://1password.com/
17 https://bitwarden.com/