

 FREEDOM OF THE PRESS FOUNDATION

<https://freedom.press>

*Protecting devices from theft,
loss, damage, and seizure*

2026 has been a wild ride. From Operation Metro Surge right here in Minneapolis to a raid seeking reporting materials in D.C., it's clear the data journalists work with needs to be protected.

And at the center of both of these stories? Laptops, phones, and other digital artifacts belonging to journalists, as well as members of the public seeking to hold law enforcement to account.

This zine is here to offer points of reflection for how we might keep our devices safe. Let's get started!

Quiz: What devices should I bring?

Do you travel internationally?

- A. Yes, I travel outside of the country on a regular basis
- B. Yep. Once in a while
- C. I very rarely travel outside the U.S.
- D. Never

How often do you report from potentially hostile situations?

- A. Fairly often
- B. Sometimes
- C. Hasn't come up yet
- D. I cover other beats

How much time are you willing to spend on device prep?

- A. I'm already on top of it!
- B. I enjoy things like this. I'll make the time
- C. I'm willing to do it, but I'm very busy
- D. I have better things to do!

Resources

A journalist's guide to digital security risk assessment

<https://freedom.press/digisec/blog/a-journalists-guide-to-digital-security-risk-assessment/>

The 2026 journalist's digital security checklist

<https://freedom.press/digisec/blog/journalists-digital-security-checklist/>

Encryption toolkit for media makers

<https://freedom.press/digisec/guides/encryption-toolkit-media-makers/>

Ask a security trainer: How do I get secure phone backups?

<https://freedom.press/digisec/blog/ask-a-security-trainer-how-do-i-get-secure-phone-backups/>

Smartphone security guide

<https://freedom.press/digisec/blog/your-smartphone-and-you-handbook-modern-mobile-maintenance/>

How to limit exposing your location

<https://freedom.press/digisec/blog/how-to-limit-exposing-your-location/>

Brought to you in part by The Digital Security Digest, a weekly newsletter with security tips that keep you, your sources, and your devices safe.

Sign up today!

Dispatches released weekly.

 FREEDOM OF THE PRESS FOUNDATION

**BECAUSE WE
KNOW SECURITY
IS IN THE NEWS**

FPF.TRAINING/SUBSCRIBE

Before you go...

A few housekeeping tips to take care of just before you leave home:

- Log out of accounts you do not want accessible to others, and sign out of sensitive chats
- Ensure that a friend, relative, or colleague is aware of your whereabouts, and provide them with an update as soon as possible afterward
- If you are not using your device(s), power down entirely. This will enable disk encryption, and make it harder for someone to analyze your device

Rapid response

If the situation requires it, be prepared to quickly power down in order to let FDE take full effect.

On an iPhone:

- Option 1: Hold down the power button and the volume up button at the same time
- Option 2: Swipe down from the top-right corner of the screen. Tap and hold the power button the top right corner

On an Android:

- Hold down the power button. Tap the power icon on the bottom left. Either “Power off” or “Lockdown”

To quickly power down your computer:

- Hold down the power button for about 10 seconds
- Unplug any peripherals

How easily could you get your hands on another device?

- A. I may have one lying around
- B. I’m about to upgrade soon, so...
- C. Honestly, I haven’t looked into it
- D. Do I really need to? I don’t cover anything intense

What’s your technology budget look like?

- A. I may be able to expense it
- B. I can spring for a refurbished device
- C. If I save up, maybe I can justify a tech-related expense...
- D. My what?

If you answered mostly As or Bs: Consider a special-purpose phone and laptop so that you can leave your everyday device at home.

If you answered mostly Cs: It may be worth creating and using a “clean” disk image for your everyday phone or laptop before you travel or attend a protest, if you can’t leave it at home.

If you answered mostly Ds: So long as you keep things low-key and also adhere to digital security baselines like keeping your phone and laptop updated, dialing in your settings, using strong passwords, and taking sensitive conversations to Signal, you should be safe to use your everyday device without too much extra effort.

Cryptoquote

"E'ra hawnjaz pdwp laklha sehh bkncap sdwp ukq owez,

laklha sehh bkncap sdwp ukq zez,

xqp laklha sehh jaran bkncap dks ukq iwza pdai baah."

– IwuW Wjcahkq

Using your everyday device?

Starting by making a backup

Access to information is one of the most important elements of digital security. The 3-2-1 rule from preservation experts offers guidance for ensuring access to backed up data:

- 3 total copies of your data
- ... stored on 2 different types of storage media
- ...with 1 copy kept securely off-site

Cloud backups

Backing your data up to the cloud is sufficient for many. It's already a step up from exposing sensitive info to physical risk. But, as a journalist, it's important to ask yourself a few questions before stashing your data in iCloud or Google or Microsoft OneDrive or DropBox or et cetera:

- Is there any risk of your provider receiving a legal request to access your data? (Google receives roughly half a million requests for user data every six months from the feds, for example)
- Are you comfortable storing sensitive data about yourself and others with third parties on servers you don't directly control?

For additional safety, if you're an Apple user, you can encrypt much of your data with **Advanced Data Protection**. That said, Apple can still conceivably turn over your data in response to a legal order, even in its encrypted state, and government actors may operate under a "harvest now, decrypt later" strategy. In other words, just because a government actor might not presently have the keys necessary to decrypt your data, that might not be true in the future.

To get to the point: If you have access to extremely sensitive data, it is still worth figuring out how to keep that data close to home.

Information to have handy on longer trips:

- ☐ Digital copies of IDs / important documents
- ☐ Important contacts (your boss, your lawyer, your family)
- ☐ Addresses for places to turn if you need help
- ☐ Unless you can print: Your travel itinerary / downloaded maps
- ☐ _____
- ☐ _____

Secondary accounts, as needed:

- ☐ Email (gmail, protonmail, etc)
- ☐ Signal

Mobile apps 

- ☐ Password manager
- ☐ Private browsing
- ☐ Two-factor authentication
- ☐ Secure messaging and calling
- ☐ Travel-specific resources (e.g. ride share, AirBnB)
- ☐ News, games, entertainment
- ☐ _____
- ☐ _____

Software 

- ☐ Password manager
- ☐ Private browsing
- ☐ Email and file encryption
- ☐ Secure file sharing app or website
- ☐ _____
- ☐ _____

- ☐ Disable notifications. Go to Settings > Notifications > App notifications
- ☐ Enable Advanced Data Protection to prevent unauthorized devices from connecting. Go to Settings app > Security and Privacy > Advanced Protection

Contact Freedom of the Press if you'd like to get deeper into hardening your devices.

Install (or keep) only what you need

We've made it this whole time without writing the words "it depends" but we can't hold back any further. Deciding what apps and software to bring with you comes with a hefty dose of "it depends on your situation."

For instance, you may need to stock your device with a password manager if you're traveling (check out Travel Mode in 1Password if you haven't already!). But if you are headed on a reporting trip for the day, you might prefer to log in to your accounts in advance so that you don't place your password manager at risk.

Use the list on the next page to start your prep, and feel free to cross out anything irrelevant.



Encryption factoid! While held under arrest, Mary, Queen of Scots (left) communicated with her collaborators using ciphertext that included Zodiac symbols to replace letters.

By 1571, Queen Elizabeth I's formidable intelligence network had learned of a plot against the queen coordinated in this manner, ultimately leading to Mary's downfall.

Local backups

External drives are great for this – especially when you encrypt them! - as are password-protected laptops and desktop computers. Just remember to set them up with a strong password, and power them down when you want all that data to be fully encrypted.

How to encrypt an external hard drive

Directions for macOS computers

- ☐ Go to the Disk Utility app
- ☐ Choose View > Show All Devices
- ☐ In the sidebar, select the storage device you want to encrypt
- ☐ Click the Erase button in the toolbar
- ☐ Enter a name for the volume
- ☐ Click the Scheme pop-up menu. Choose your preferred format
- ☐ Click the Format pop-up menu. Choose an encrypted file system format
- ☐ Enter and verify a password, then click Choose
- ☐ Click Erase, then click Done

Source:

<https://support.apple.com/guide/disk-utility/encrypt-protect-a-storage-device-password-dskutil35612/mac>

Advice for all devices

Ideally, you'll have arrived at this point with a "clean" device: one that doesn't contain sensitive information about you or anyone you communicate with. This is a great time to get your device set up for extra protection.

Update your devices and your apps

Start by ensuring that your device is fully up to date. Same goes for apps and software. This will help you ensure that known vulnerabilities have been patched.

Make sure that Full Disk Encryption is turned on

FDE encrypts your data when your device has been either powered off or restarted, before you enter your passcode.

FDE for phones is enabled by default on iOS and modern Androids with a passcode.

As for FDE on computers:

- If you use macOS, turn on FileVault
- If you use Windows Pro, Enterprise, and Education editions, set up BitLocker
- If you don't have these fancy Windows editions, consider upgrading, or use VeraCrypt

If you are part of a mixed group of device types, use VeraCrypt for interoperability.

Set strong passwords

It really can't be overstated: make sure your password is unique, random, and long. Consider an alphanumeric password for phones and computers alike.

On the note of passwords: When you set up FDE or encrypt a drive, you are likely to also come into possession of a password specifically to access the data that's being encrypted. Store that password somewhere safe: in your password manager, on an encrypted drive, or printed out and stored somewhere in your home.

Adjust your settings

Take a tour through your settings app to make sure your device is set up in a security-forward manner.



iPhone security settings:

- ☐ Review your connection settings. Turn off Wifi and Bluetooth unless you plan to intentionally connect to a network
- ☐ Disable notifications. Go to Settings > Notifications > Show Previews
- ☐ Disable biometrics. Go to Settings > Face ID & Passcode > iPhone Unlock
- ☐ Enable Stolen Device Protection. Go to Settings > Face ID & Passcode > Stolen Device Protection
- ☐ Enable Lockdown Mode to prevent unauthorized devices from connecting. Go to Settings > Privacy & Security > Lockdown Mode



Android security settings:

- ☐ Review your connection settings. Turn off Wifi and Bluetooth unless you plan to intentionally connect to a network