

WITNESS




SEE IT


FILM IT

CHANGE IT

[Donate](#) [Tools](#) [Tactics](#) [How-To](#) [Ideas](#)

· MENU 

 Tweet this  Share  Read later

 Posted on Archiving Human Rights, Internet Shutdowns, Tactics, Tools, Video for Change

Backing Up Phone Media Without Internet or a Computer

Documenting During Internet Shutdowns series

By Yvonne Ng



This post is part of a series on [Documenting During Internet Shutdowns](#).

Also available in [Arabic](#), [Spanish](#) and [Bahasa Indonesia](#).

With contributions by [Arul Prakkash](#)

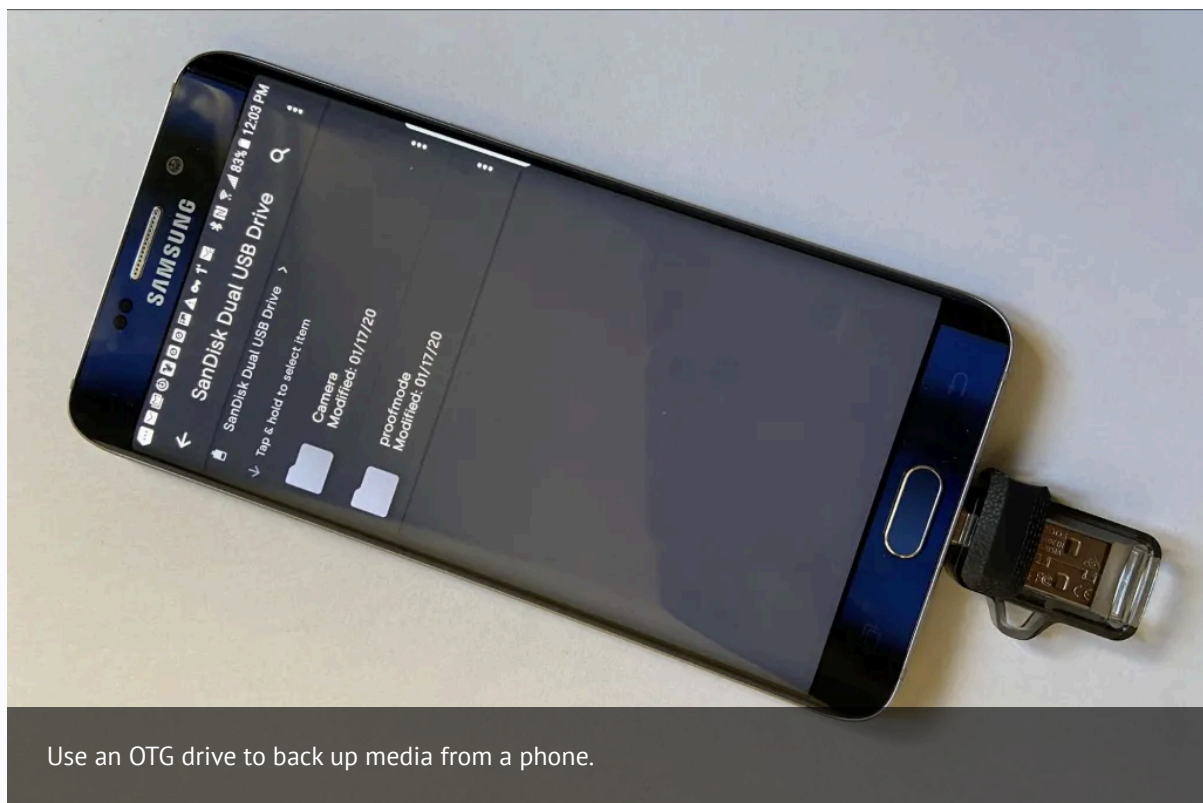
Last reviewed: 31 January 2020

[Backup](#) is key to ensuring your data and documentation are not accidentally deleted, corrupted, or lost if your device is confiscated. During an internet shutdown or slowdown, you might not be able to run your regular cloud backup or send your documentation to a safe offsite location. Offloading to a desktop or laptop computer is one way to back up, but since people often do not have access to one, here are some options and tips for backing up your media from your phone during an internet shutdown without a computer.

Use an OTG or wireless drive

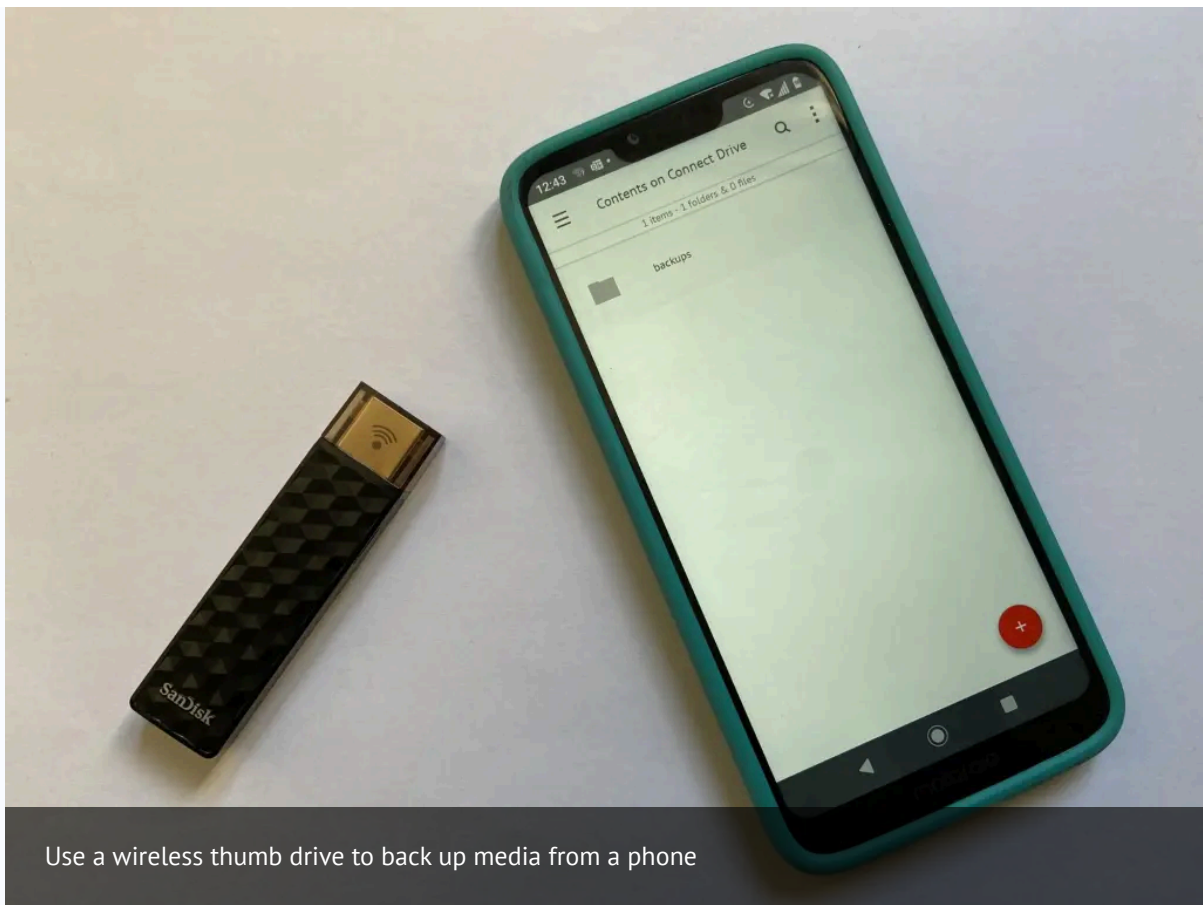
OTG, or on-the-go, drives are a type of USB drive compatible with many (but not all) Androids. You can plug an OTG thumb drive directly into your phone, or use a OTG-to-USB adapter to connect your phone with a regular USB hard drive. With OTG, your phone provides the power for the drive.

Popular brands of OTG drives include SanDisk, Kingston, and Samsung, although there are many others. They typically cost between US\$8-\$25 depending on the storage capacity.



Wireless thumb drives / hard drives are similar to regular hard drives except that they do not require cables. This allows you to connect devices that don't normally connect to hard drives, such as your phone. An advantage of a wireless drive over an OTG drive is that you can connect multiple users to the same wireless drive at once. This can be useful, for example, in a protest situation when you are filming as a team — everyone's footage can be backed up to a hard drive that another team member is carrying. Note that because they are not drawing power from a device, wireless drives rely on battery power and need to be charged.

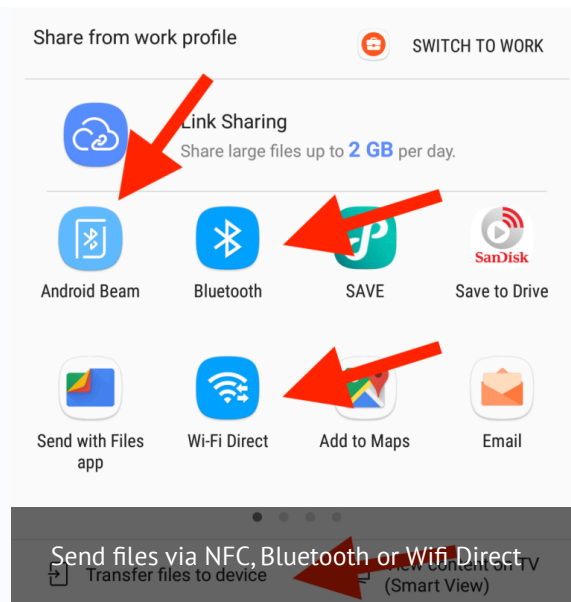
SanDisk is probably the most popular brand of wireless thumb drives, although there are others. Wireless thumb drives are generally more expensive than OTG drives, and range from about US\$25-\$100 depending on the storage capacity. Larger wireless external hard drives start at around US\$150 depending on the storage capacity.



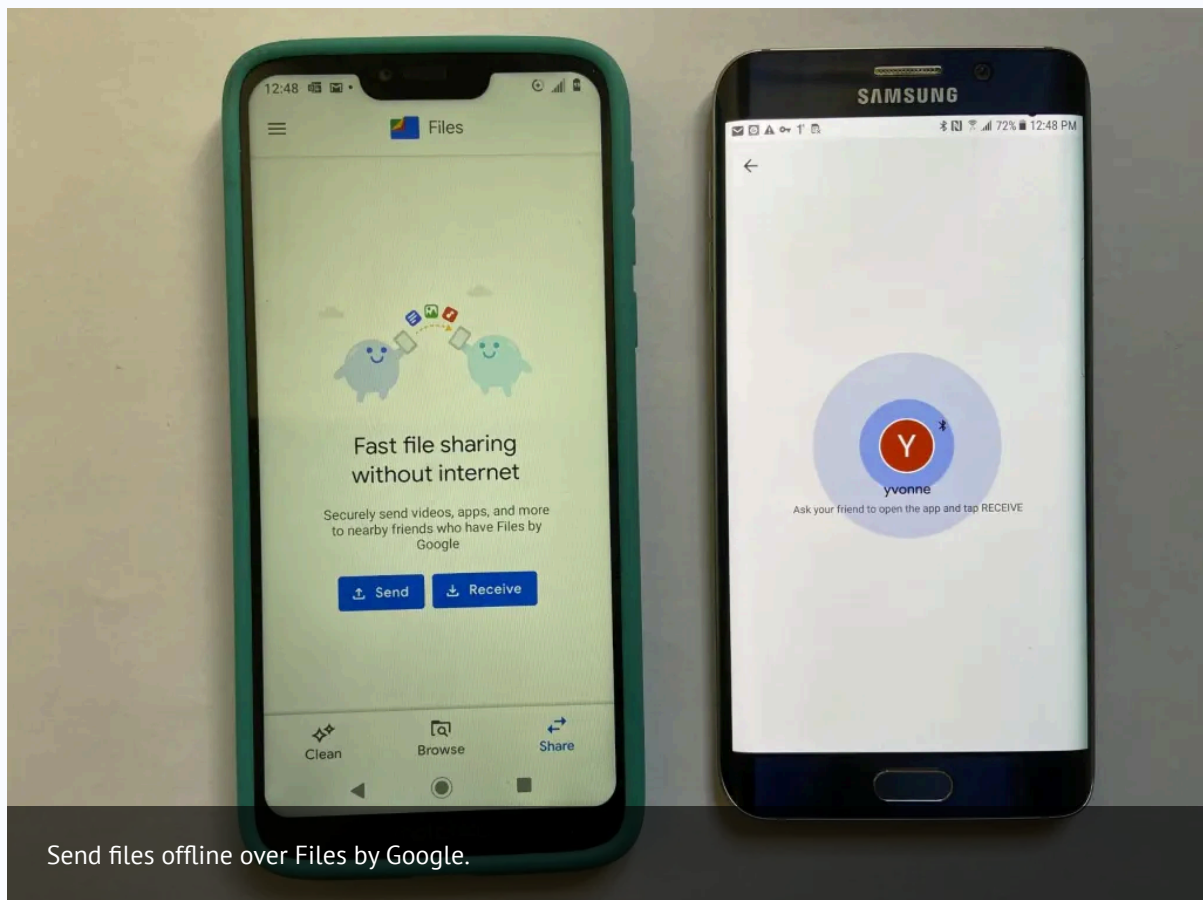
Use a wireless thumb drive to back up media from a phone

Alternative: Use an old unused phone

If you don't have an OTG or wireless drive, but you have an old phone that still works that you no longer use, you can also re-purpose it for backup. As long as both phones are in physical range, you can connect and copy media from one to the other using Bluetooth, WiFi Direct, or Near Field Communication (NFC) / Android Beam. Bluetooth and Wifi Direct are both wireless technologies that can “pair” two devices without another router or access point in between. WiFi Direct provides a wider range and faster data transfer than Bluetooth, but uses up a lot more power. Meanwhile, NFC has a much shorter range (~4cm) and much slower transfer speeds than either Bluetooth or WiFi Direct, but connects faster and uses less power, so can be useful for quick small transfers when you have both devices in hand.



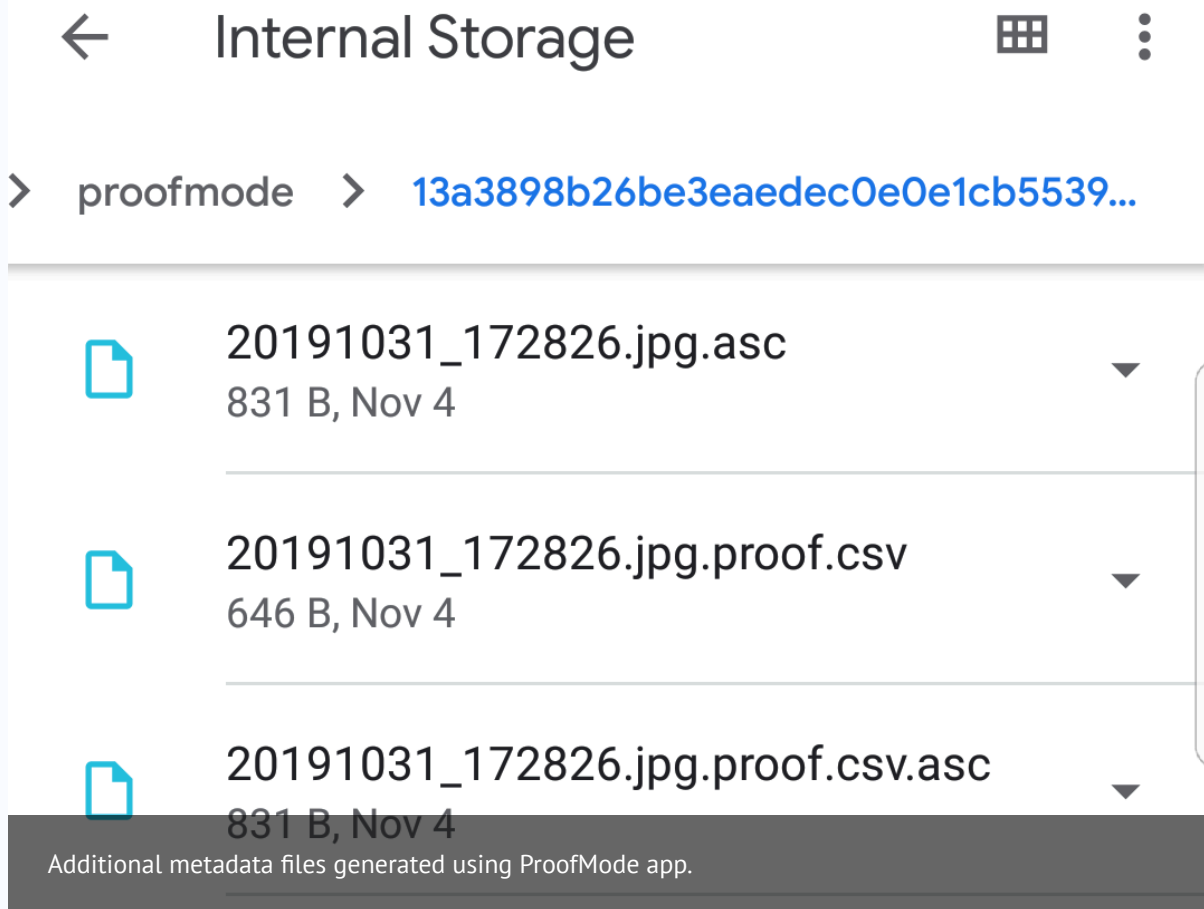
Your phone probably has built-in Bluetooth, WiFi Direct, or NFC apps / features that allow you to choose nearby devices to share with. If both phones have Files By Google installed, you can also share files offline using these technologies within the app.



Important: the downside to the ease of connection provided by these services is that they are not secure. Bluetooth and wifi beacons/scanners can be used to trace your location or probe your device for information. Infiltrators may try to pair with your device, send you unwanted files, or even gain control of your device if it is vulnerable. **To be safer, turn these services off when you are not using them and only turn them on when you're in safe locales, limit app permissions to only what/who you need, and practice good phone security like running updates and having a strong passcode.**

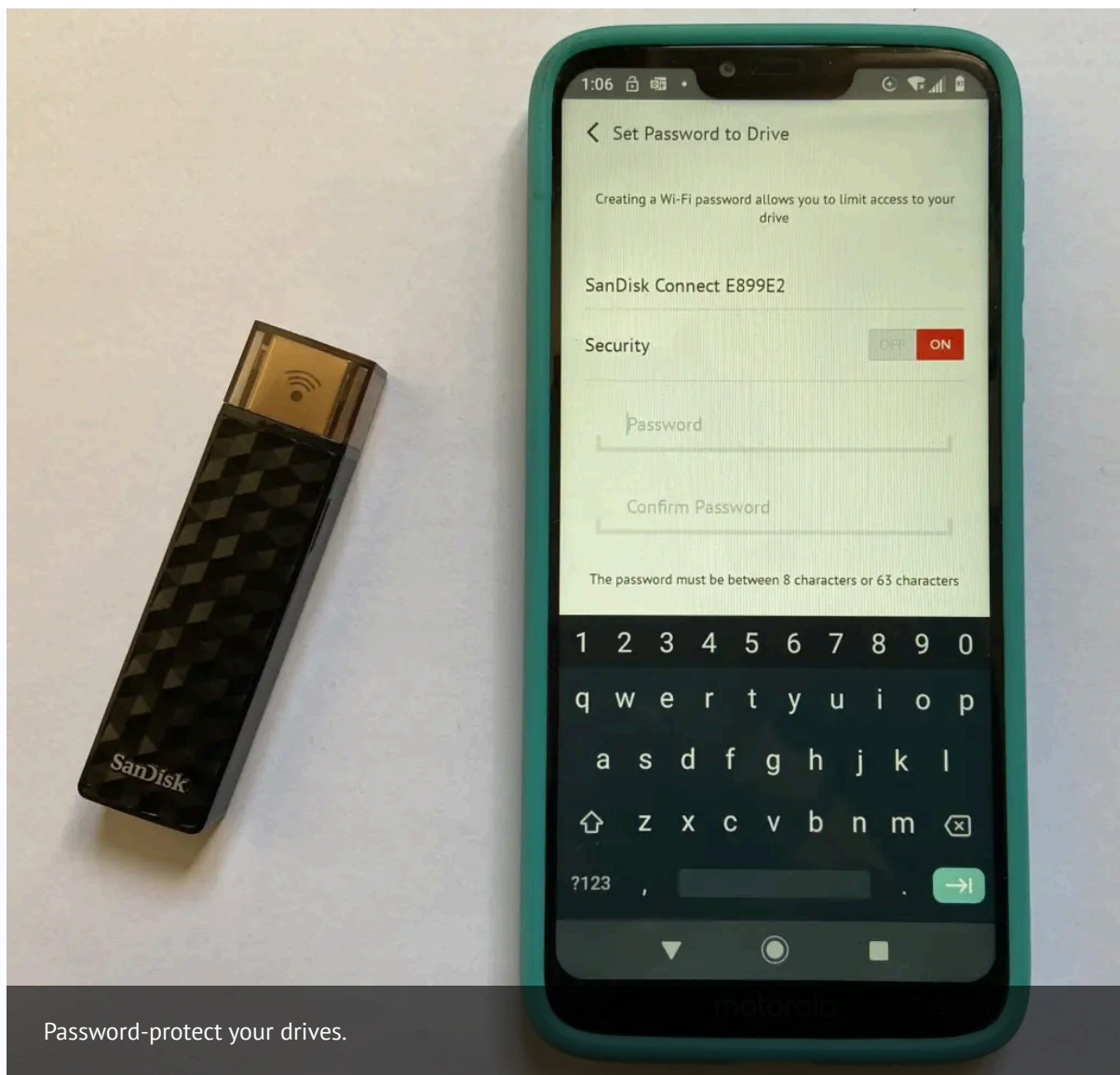
Include any separate description / metadata

When copying media to an OTG drive, wireless drive, or an old phone, it is useful to include any descriptive information or metadata that may be separate from the media. Many [documentation apps](#), for example, generate CSV or JSON text documents that include metadata pulled from the device (e.g. geolocation, time, date) and any description manually inputted by the user. Make sure to export and include these metadata documents in your backups too.



Password protect the drive

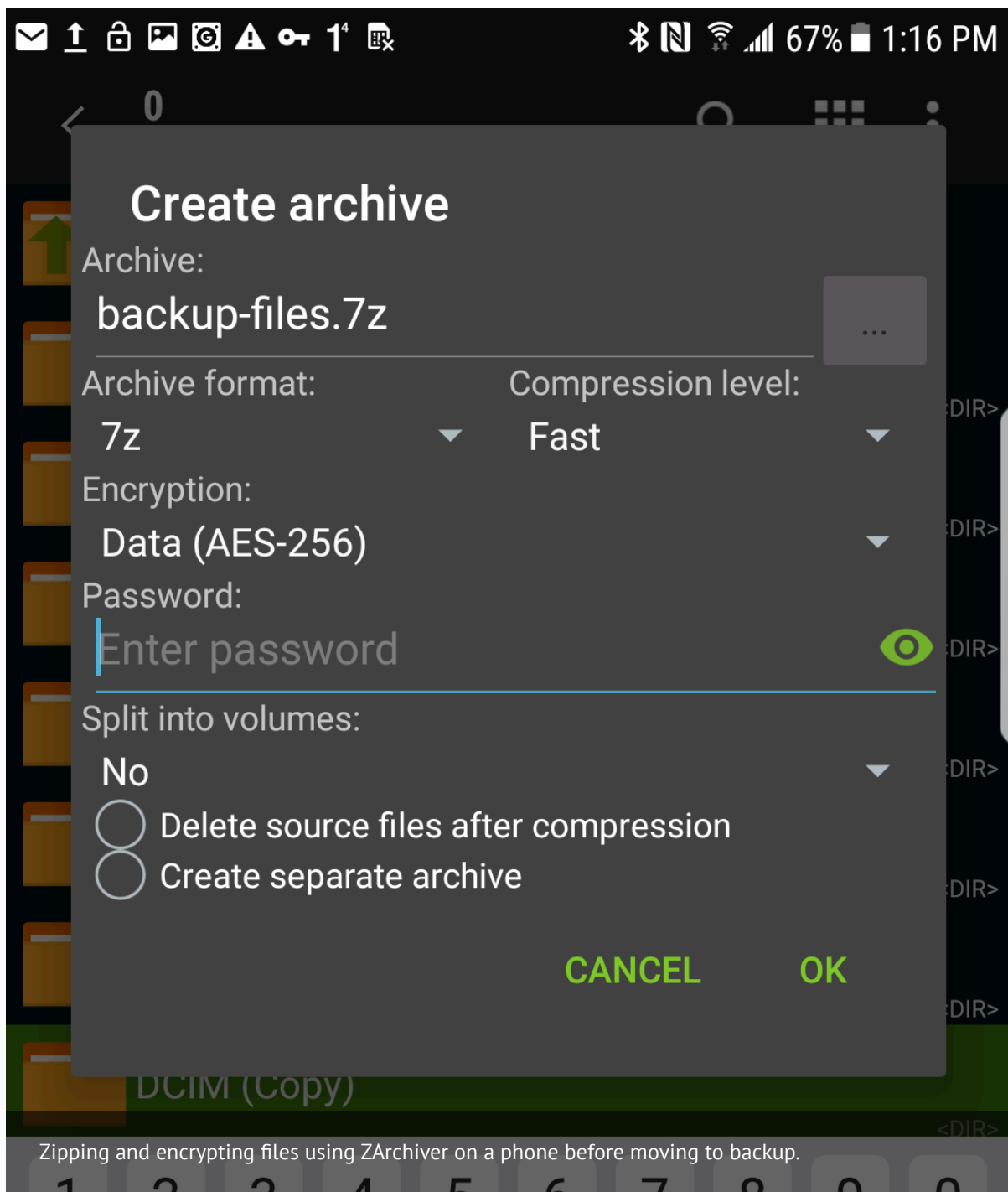
Many wireless drives can be password-protected with a mobile app that comes with the drive. Note that password-protection is not the same as encryption (see below). Most wireless or OTG drives do not enable full-disk encryption using only a mobile phone, although they may be full-disk encrypted using a computer.



Password-protect your drives.

Consider encrypting the files

If you need to store your files more securely, you might consider encrypting your backups. While you may not be able to encrypt most wireless or OTG drives with a mobile phone, you can encrypt the files themselves before you move them onto the drive. Some apps that can encrypt files on Android include [ZArchiver](#), and [RAR](#). Be aware that you must remember your encryption passwords. There is no way to recover encrypted files if you lose the password.

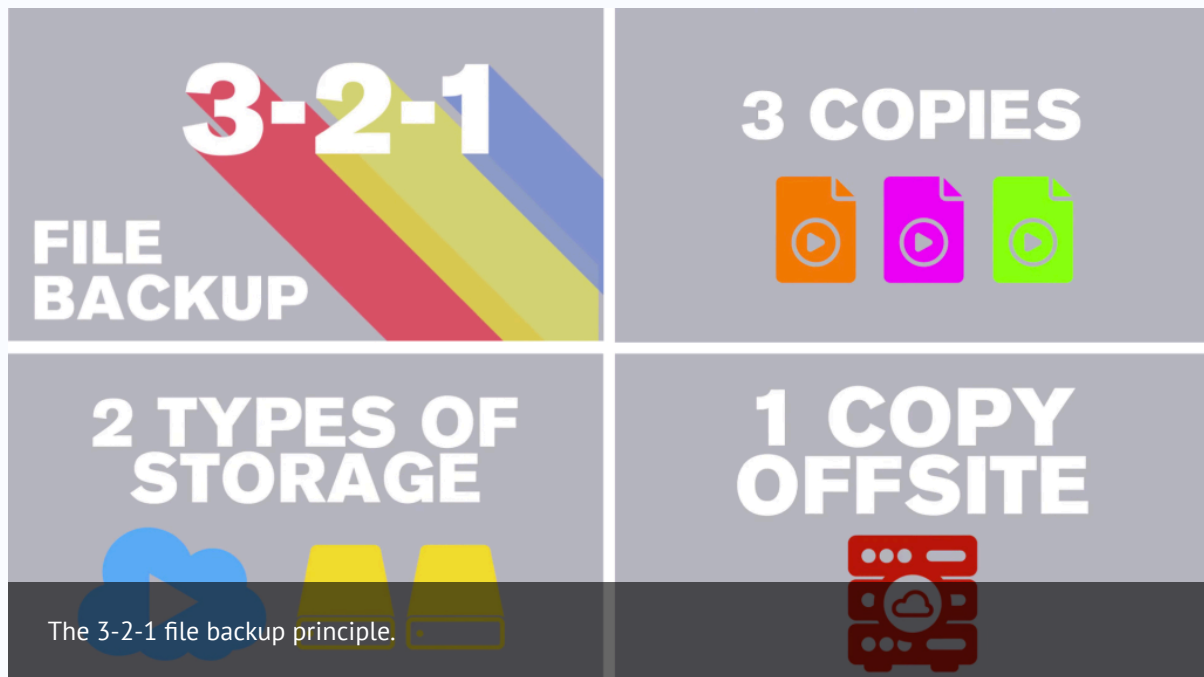


Ziping and encrypting files using ZArchiver on a phone before moving to backup.

Keep in mind that some countries may have laws that restrict or criminalize the use of encryption. Using them to prevent authorities to accessing your data may be seen as destroying evidence or obstructing an investigation, and may be punishable as a crime. This [2017 map](#) may be outdated but provides a good starting place if you have questions about the laws in your country.

Make 2 backups in separate locations.

A single backup is not always reliable. For example, you might lose the backup device, damage it, or it might just randomly fail. IT experts usually advise people to have 2 backups (i.e. 3 copies total), on separate devices kept in separate locations. This helps mitigate the variety of risks to any one particular copy.



Check out the final post in this series, [“File Sharing and Communication During an Internet Shutdown.”](#)

🌿 Archived in [Archiving Human Rights](#), [Internet Shutdowns](#), [Tactics](#), [Tools](#), [Video for Change](#) and tagged [backup](#), [internet shutdowns](#).

🔗 Share this article: [f Facebook](#) [🐦 Twitter](#)