



Looking for help? Contact us!

You may have some specific needs and questions on this topic, and we're always here to help reporters and news organizations around the world. If that sounds like you, contact our trainers for assistance.

freedom.press/training/request-training



Your smartphone & you

A tiny handbook to modern mobile maintenance

Read more! fpf.training/mobileguide

2025 Edition [CC BY 2.0]

Remix to your heart's desire.

What's the big deal?

2

If you have a smartphone, it's likely that you store information about nearly every part of your life on it. Keeping your information safe depends on learning a little more about how to choose your small computer, and how to care for it long term.



There are a few simple things we can do to keep our devices, and our information, as safe as possible on our little computers.

Set a strong password

3

If your device is ever stolen, or seized, a predictable password (e.g., "000000") makes it easy for someone to unlock your device without your consent. Consider strategies to make your password less predictable:

1. Numeric PINs (0-9) offer a very limited range of possible combinations. Instead, consider an *alphanumeric* passcode.
2. Consider a passphrase. A randomly-generated one is hardest to guess (e.g., "gate rewind"). Visit eff.org/dice to learn how to make a truly random passphrase.

Upgrading your password is easy.

Android users: Open *Settings app* > *Security & privacy* (or "Security") > *Lock screen*

iPhone users: *Settings app* > *Touch/Face ID & Passcode* > *Change Passcode*

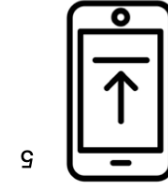
Protect data on your phone

4

If your device leaves your possession, the data can be read or copied. Fortunately it's easy to protect the data on your disk so that it's only readable after you enter your password.

iPhone users: If your device is password-protected, your disk is already encrypted — just lock your phone. **Android users** (may be different, depending on your version): Most modern Android devices, such as those in the Pixel line, are encrypted by default. For others, it's easy to encrypt your device. Go to your *Settings app* > *Security & privacy* > *Encryption*

Note that disk encryption is activated after powering off the phone. This means that solely putting the phone into sleep mode won't activate disk encryption.



5

Hackers, companies, and governments are always on the lookout for security vulnerabilities. Some bad actors will use vulnerabilities found in the software on our phones to steal our personal data. Security teams at companies like Google, Microsoft, and Apple scramble every day to put out these fires through security updates. Your phone is probably nudging you about updates for apps and for the device itself. We often treat updates as something that gets in the way, but the opposite is true; updates should give us reassurance that our devices are safer, allowing us to focus on the things we care about. Always stay updated.

Android users (may be different, depending on your version): Open *Settings app* > *Apps* > *Security & Privacy* & *Security*

And every once in a while, remove those you don't need any more.

Make regular backups

7

It happens to the best of us: Our devices are lost, stolen, or broken, along with our data. Make occasional backups of these files to avoid this cruel fate. There are free and easy tools for remote backups like iCloud and Google Drive, which by default store your data in a way the company can read, making it more vulnerable to legal requests, as well as hackers. If these risks are too great and you have a computer, consider storing backups there instead. **Android users:** On a Windows computer, connect to your phone through USB. Search for your Android device on File Explorer. Drag and drop your phone's files to your preferred location on your computer. On a Mac, you will need to transfer files over through a USB thumb drive. **iPhone users:** On your computer open *Finder* or *iTunes* > [iPhone name] > *General* > *Backups*