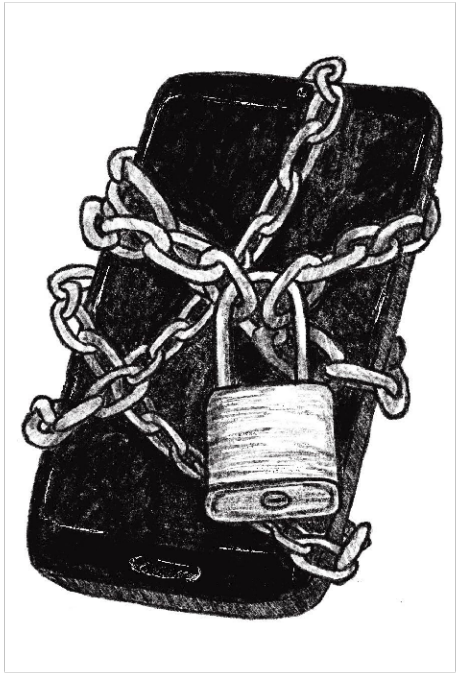


KEEPING SAFE

Easy tips to secure your phone

https://distro.f-91w.club

We all use smartphones. They're useful and fun, but they also hold a ton of information about us and our social networks. If your phone falls into the hands of someone who wants to hurt you and your friends, your smartphone can become very dangerous. Your phone can be stolen (or "seized") by such people under a number of circumstances.

Widespread message encryption has meant that it's harder to access people's private communications—often the easiest way to do so is to get physical access to the device. If bad people want to access information or messages on your phone, they will most likely rely on stopping and detaining you and confiscating your phone—if they have the resources to do so.

For example, in the recent wave of arrests targeting Palestine solidarity activists in Toronto, police conducted early morning house raids to arrest people and seize their phones and other devices. They may use what they find in those phones to criminalize more people.

This is a scary situation, but we aren't powerless. ***Don't be intimidated, don't be afraid to be political and organize publicly.*** Just know the risks you are taking, and protect yourself and the people around you by considering these simple tech and behaviour based steps.

It's not all or nothing—you don't have to do everything we suggest here—but the more you can do, the better.

We keep ourselves safe.

So your phone was taken from you...

Once you are free and able, there are a few things you can do to mitigate the harm:

- On a different device, revoke all your sign-in sessions from services (like Google, iCloud)
- As quickly as you can, go get a new SIM card, transfer your number, and register for all the apps you commonly use on a new phone. For Signal, this will mean your old phone will stop receiving new messages meant for you.
- For WhatsApp, once you set up a new primary phone, you can log out all other devices.
- You should then change all your passwords, including for social media accounts.

However there is only so much you can do. All the data on your phone might be copied off it and analyzed, and you can't change what was available at the time the phone was taken (unless you manage to perform a remote wipe very quickly, which could get you in more trouble). ***This is why all the preventative measures here are so important!***

If your phone was taken and then returned to you, you should not continue using it since there is a good chance that it has been compromised. You should consider all data on it to be lost and just replace the phone (much easier to do if you have some good up-to-date backups handy!)

Keep Organizing

Keep Yourself Safe

Be Ready to Protect & Defend Each Other

Be Ready To Win

manage to break into your phone. This is a good time to make an encrypted backup of files you want to keep but that don't need to be carried around with you on your phone!

8. Don't display messages on your lock screen

If your phone is taken from you while turned on (and therefore unencrypted), that's pretty bad. What's worse is if your phone doesn't even need to be unlocked to see new messages coming in! Imagine all your Signal group chats blowing up because your phone was taken, and the person who took it is reading every one of those messages in real time on your lock screen! You can tell Signal to omit the sender name and message content from notifications. This is set under Settings -> Notifications -> Show.

9. Leave your phone at home

Raiding houses is difficult and expensive. It's easier to take phones off people stopped on the street or detained at demonstrations or actions. If you are going out to something with that risk, it is a good idea to ***leave your phone at home***. Always err on the side of caution. Life can be unpredictable and you never know what might happen after you leave the house. If your phone is at home (encrypted and turned off), it can't be taken from you during an action. It can take some getting used to, but you are safer without your phone. This requires making plans to not rely on phones (or taking the time in advance to set up a burner phone when needed). Make plans with your friends in advance. Memorize or write down important numbers on your arm. Wear a watch. Get a paper map.

1. Encrypt your phone

Encryption means the data on your device is coded so that it can't be read without decoding it with a key.

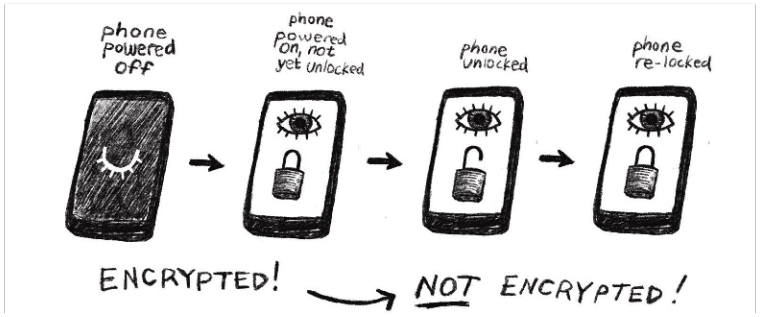
iPhone: encryption is turned on automatically if you are using a passphrase
Android: you can turn on encryption in security settings

If your phone isn't encrypted, anyone who has your phone can see its contents by copying it to a computer *even if they don't know your passphrase.*

2. Keep your phone turned off

Most phones are only encrypted *before you enter your passphrase for the first time after turning the phone on.* After that, all the data on the phone is effectively unencrypted and the lock screen just prevents someone from picking up your phone and immediately using it. If a phone is seized after it has been turned on and unlocked for the first time (decrypted), a mildly skilled hacker can access all the data by connecting the phone to a computer.

So, it's a good idea to keep your phone turned off whenever you can! Some phones have a setting that allows you to schedule times when the phone will power off—on Android, it is likely in system settings or power settings. Others even let you make the phone restart after a certain amount of time. Settings like these can help keep your data safe because restarting your phone re-enables the encryption.



If you find yourself in a situation where you think your phone is about to be stolen or taken from you, you can also attempt to turn it off.

Buy yourself an alarm clock and turn your phone off at night!

3. Use a strong passphrase

Because encryption hides your data behind a passphrase, encryption is only useful if you have a strong passphrase. A good passphrase has a mix of numbers and letters and should be as long as you can remember. Consider making a password of five or more random words plus a number. Do not use the swipey unlock feature, and do not use a passcode that's all numbers—they are easy to break.

Fingerprint or facial recognition ("biometrics") are not ideal for securing your phone, because you can more easily be forced to unlock your phone if it's locked using these methods (police are allowed to compel you to do so, for example).

I know it is inconvenient to have to type a bunch of characters each time you want to look at your phone, but it is even more inconvenient to have the contents of your phone used to lock up people you care about!

4. Use encrypted apps

Having your phone encrypted is important, but if all your messages are being sent by SMS, email, or on services that don't respect your privacy (like Instagram, Discord, or Facebook Messenger), people who want to hurt you can still get access to your messages. Signal is probably the most secure messaging app that has all the features most users expect, but WhatsApp is not bad. That said, using a secure messaging app *alone* won't help you if your phone gets captured!

5. Activate disappearing messages

Both Signal and WhatsApp have a feature that causes messages to automatically self-destruct after a defined period of time. This means that even if someone is able to access the data on your phone, they will still only get messages from the last day (or week, or whatever you set it to). There is also a setting in Signal to trim your conversations before a certain length—for example, Signal will only keep the 30 most recent messages in a chat, and all other messages are erased. This is under Settings -> Data and Storage -> Manage Storage.

6. Beware of backups

So you've encrypted your phone and are using encrypted messaging apps... but what if everything automatically backs up to iCloud or Google Drive, where it is stored unencrypted and available to anyone who can convince those services to hand it over? Automatic backups and syncing (e.g. for WhatsApp or Google) can be useful, but it means your data is being stored somewhere you don't control.

Often the easiest way for someone to bypass a phone's encryption is to send a request for data to Google or Apple, who can turn over these unencrypted backups. Disable these backup features (or at the very least, disable them for your messaging apps and contact lists) and erase the stored data if you can. It is good to make backups, but make sure they are encrypted and stored on a server *you* control, or just on your own encrypted hard drive that you store somewhere safe.

7. Delete old content

It's a good idea to go through the files on your phone periodically and delete the stuff that doesn't need to be there. This can include old chats, photos, screen grabs, notes, calendars and your browsing history. This way you are less exposed if someone does