

BASIC DEVICE SECURITY

Digital Security for Journalists and Human Rights Defenders
By Ronalyn V. Olea | Bulatlat, NUJP

DATA STORED IN YOUR DEVICES

Lost or stolen mobile devices = unauthorized access, data theft

List down all the important data in your mobile phones and/or laptops



SMART PHONES AS TRACKERS

Any phone can be tracked via mobile phone towers via triangulation and any data/SMS/calls made

Anti-Terror Act allows surveillance of computer data of 'suspects'

Prepaid or post-paid?

Do you need to carry your phone?

BASIC SECURITY

Setup a Screen Lock

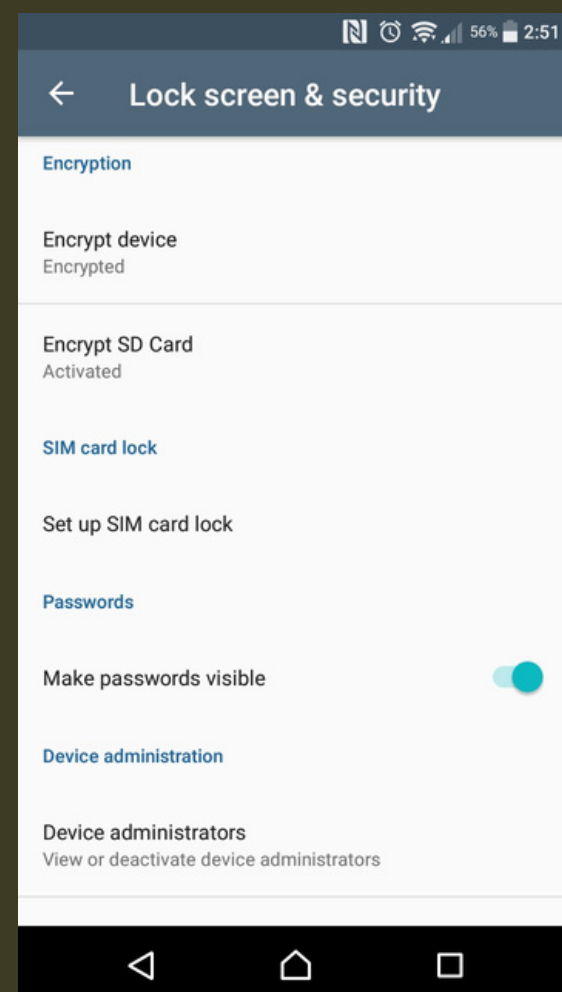
Settings-> Personal -> Security -> Screen Lock

Set the security lock timer, which will automatically lock your phone after a specified time.

Enable Lock SIM card

Settings -> Personal -> Security -> Set up SIM card lock

BASIC SECURITY



Encrypt device and SD card

Android: go to Settings, Lock Screen & Security

iPhone: go to General Settings and Set Passcode

GENERAL PRECAUTIONS

- Keep devices with you at all times. Never leave your phones or tablets out in public.
- Use a security code. Add a Personal Identification Number
- Monitor for tampering. Mark your device with something unique and not immediately noticeable to help you identify it
- Use tamper-proof security tape at the edge of devices that open easily (especially when asked to leave your cellphones)

PROTECT YOUR DELIVERIES!!!

BAKEREX the bakery exchange, inc. **TAMPER-PROOF SECURITY TAPE**



BEST FOR:
SENSITIVE DOCUMENTS
FOOD DELIVERIES
HIGH VALUE ITEMS

AVAILABLE IN 2 SIZES & COLORS
BROWN TAPE 30mm x 10 meters
YELLOW TAPE 50mm x 10 meters

EMAIL:
inquiry@bakerex.com

Grab/Lalamove etc. for Account of Buyer

GENERAL PRECAUTIONS

- Keep your IMEI (International Mobile Equipment Identity) number separate from your phone.

- helps you trace and prove ownership if your phone is stolen. Reporting it to service providers will block the device.

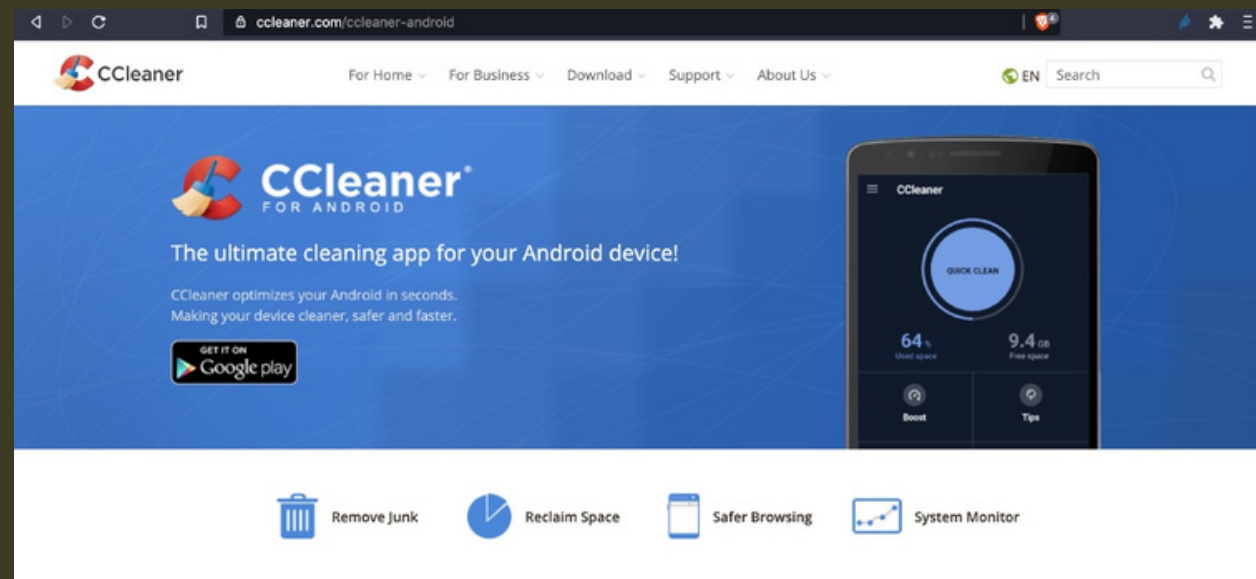
To find your IMEI:

Key *#06# into most phones

Look behind the battery

Check the phone settings

GENERAL PRECAUTIONS



- Install anti-virus. Some phones have their own AV. (Avast, BitDefender, Malwarebytes, Avira etc.)
<https://fossbytes.com/best-android-antivirus-apps/>
- Install CCleaner for Android to delete files and clean digital footprints.

BASIC SECURITY

- Keep your software updated.

Settings -> About phone -> Updates -> Check for updates

- Turn off Wifi and Bluetooth by default. Ensure that Tethering and Portable Hotspots are switched off when not in use.

Settings -> Wireless and Networks-> More -> Tethering and mobile hotspot






- Backup the contents of your phone regularly. Use encrypted devices (SIM, OTG, hard drive)

MOBILE APPS

Mobile apps can pose serious threats. Malicious apps can spy on your device, collect information about your activities, read your messages, or copy and send information from your phone to a remote server.

- Download apps from official app stores.
- Limit the number of apps you install to the bare minimum and install apps you need only.
- Review your existing apps permissions and disable all permissions to your location, camera, contacts, messages and mic unless needed for the apps to work. Choose to disable these permissions and enable only when using the app.
- When installing a new app, make sure it is from a legitimate developer, examine the app permissions. Check the app history and when it was last updated.

SECURE COMMUNICATIONS

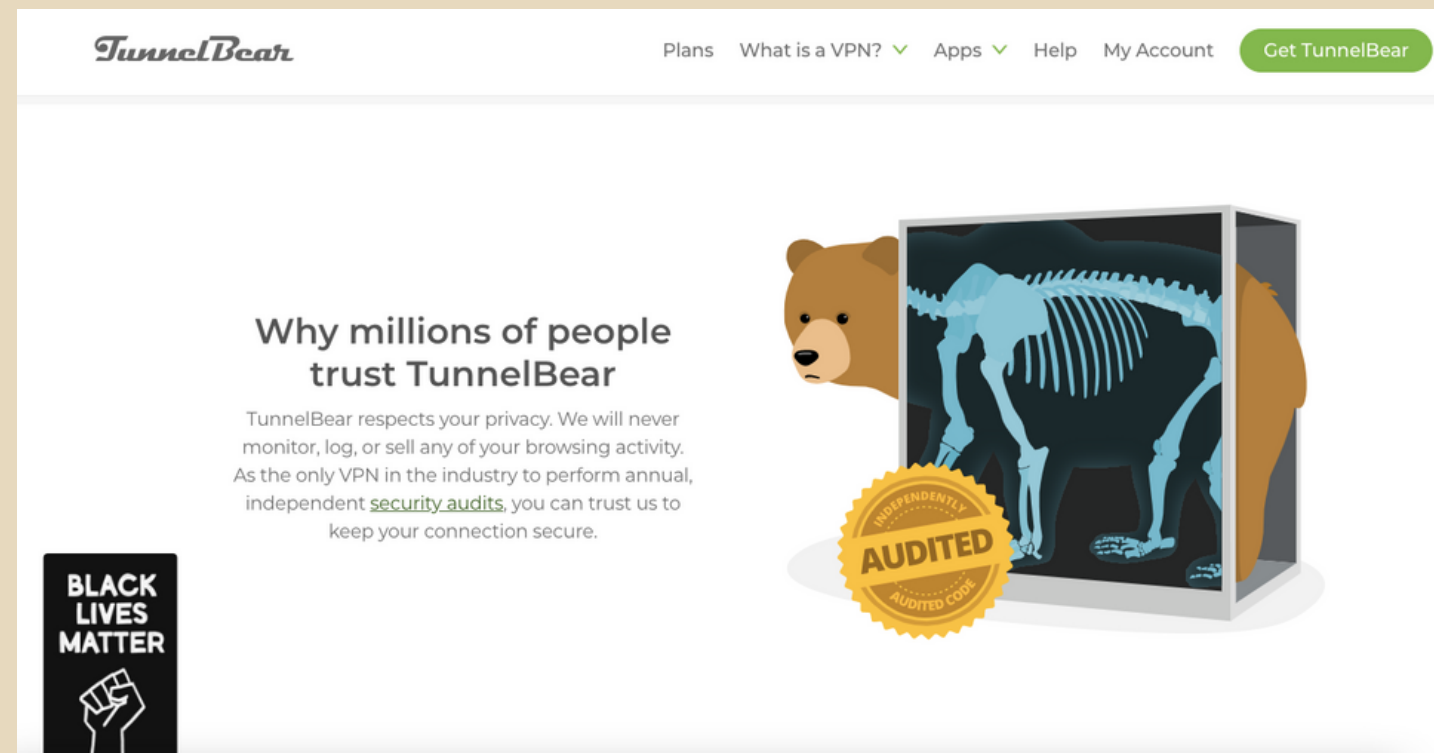
| | | |
|--|---|---|
|  |  |  |
| Whatsapp <ul style="list-style-type: none">+ End-to-end encryption+ Easy to use- Breaches- Metadata go to Facebook | Telegram <ul style="list-style-type: none">+ End-to-end encryption+ Good when the internet connexion is slow- Breaches | Signal <ul style="list-style-type: none">+ End-to-end encryption+ Collecting minimal metadata on users datas are stored in your device, not the cloud+ Get your messages deleted- Not always stable |
|  |  |  |

- Do not autosave your username and passwords
- Use Signal for encrypted communications

<https://www.securemessagingapps.com/>

- Use the internet securely

SECURE COMMUNICATIONS



The screenshot shows the TunnelBear website homepage. At the top, the TunnelBear logo is on the left, and navigation links for 'Plans', 'What is a VPN?', 'Apps', 'Help', and 'My Account' are in the center. A green 'Get TunnelBear' button is on the right. The main content area features a large illustration of a brown bear with a blue skeletal overlay, standing on a grey base. A gold seal with the word 'AUDITED' is positioned in front of the bear's legs. To the left of the bear, the text reads: 'Why millions of people trust TunnelBear'. Below this, a paragraph states: 'TunnelBear respects your privacy. We will never monitor, log, or sell any of your browsing activity. As the only VPN in the industry to perform annual, independent [security audits](#), you can trust us to keep your connection secure.' In the bottom left corner, there is a black square with the text 'BLACK LIVES MATTER' and a white fist icon.

- Use VPN (Tunnelbear, Psiphon, ExpressVPN, ProtonVPN)
- Do not connect to a public Wifi

LAPTOP



- Set a non-admin account & use for daily use
- Set a strong password
- Install and update AV (Avast, Malwarebytes)
- Never leave your computer unlocked
- Keep OS and software updated
- Encrypt part of your hardware
- If you connect to a public wifi, use VPN