

Anonymous Tor Phone

HOEK 🏠 2023-05-02 🔄 2023-05-02 | 📖 guides | 💎 anonymous phone, privacy phone, secure phone, tor phone

I was always curious about all that bad guys (criminals, drug dealers, hitman's, thief's etc.) using not very good and secure communication channels. Forgetting about whole OPSEC stuff. There is a lot of stories about mafia or other criminals where people get caught because of mobile phone tracking, or because using unencrypted communication. I understand this is part of society with no good education, or technical knowledge, but why they do not hire some nerd to configure them whole environment? Of course there are stories where for example "IT guy" configured secure communication using BlackBerry smartphone for El Chapo and his "friends". But everyone can make a mistake, or just take bribe, or becomes a witness in exchange for a low sentence. There is a lot of stories like that. In such a case I would use a technique from Egypt, anyone building my pyramid would be eliminated upon completion of the contract ;)

There are also stories when feds get access in legal/illegal way to some app and could track owners. Example: EncroChat. Funny right?

In today's world smartphone function like calling or sending SMS is probably last function of the phone that is checked, as it is probably main function which is used last. I guess it also depends on country, region, age, gender and many other stuff, but in most very well developed countries probably sending SMS or calling someone is last option. So criminals are probably last guys on earth who should call or SMS each other.

For example me, since I configured spam protection in my mobile phone I do not remember when someone called me last time. Funny is that I even forgot how my ringtone sounds. When my phone is ringing I am not sure if this is mine, or someone else, and I need a minute to realize that - oh shit it is my phone!

I communicate with my friends, and family mostly using some kind of chat apps like, Telegram or Signal, when I am on holiday I am using WhatsApp (as in some countries it's almost like official national app). So messages and calls are over the Wi-Fi or Mobile Data using third party apps. Rest communication is using some platforms or emails. Each company like Internet provider, electricity/gas company, bank etc. has own websites, online forms, emails and apps. I really do not remember when I had to call someone.

I thought ok, what if I would be a criminal, with IT knowledge, and how would I organize my communication, with my gang members, customers or contractors? I know it depends very much of customers and type of organization, as if I would be a drug dealer teaching a junkie how to use PGP encryption I would probably have no clients :) but let say in general, I would like to have a device, smaller than a laptop, to have possibility always check my communicator app and email. Smartphone is probably best option. Everything encrypted and torified.

In this article I will describe how I configured my test smartphone to make it as much as possible secure, with some OPSEC steps in the background like avoid follow the money track or password security. I guess many readers may found some issues or mistakes, but hell yeah, please share them in the comments as I would love to know where I did a mistake. Maybe I could update this article in the future to make all steps even more secure.

Of course I didn't invented or discovered anything new. I just setup phone, using various existing solutions and put it into one instruction. It's just a smartphone with custom rom and app to torify whole traffic. Don't expect magic.



Choose a system

Definitely we need a custom, actively developed, updated system. Custom rom to choose are LineageOS, E, GrapheneOS, CylaxOS, Replicant, DivestOS, and if you Google some Android alternatives focused on privacy you will find much more.

I trust LineageOS, I bring back to life a lot of old smartphones that was not updated anymore by official brand, and was still good enough to use. I used it even in the past when it was called CyanogenOS. This project is mature, and never had any big security problem. Of course you can do your own research and choose whatever you want.

Choose and buy a phone

Choosing a phone is easy, you just need to pick up one supported by your custom rom developer. In my case I choose one from this list. I was looking for something fast, small and not very expensive. Google Pixel 3, was best choice.

Now important part of getting the phone, is to buy it in the way that no one can connect you with the transaction. Remember? We are bosses of the criminal world, we can use our magical power, and someone will buy it for us. But when we are on our own, we can find some homeless guy, and for bottle of whisky tell him to buy it for us in some pawn shop, or buy it using stolen cards, bitcoins, far away from home etc. I mean options for buying something for cash or build a fake identity profile is easy these days. With fake ID we can register some crypto debit card, and exchange our bitcoins to USD, and pay in online shop sitting behind Tor and VPN, with delivery to some fake spots, or pickup machines, where another jake for money can pick it up for us, to avoid street/shop/pickup points cameras. Holy shit, what a story. Yeah, but this is another story for another article, we should focus on main steps.

Don't forget to buy one with unlocked OEM. To have possibility install custom rom's. Sometimes phones are sold by some brand like Verizon or something and are locked.

I bought mine on AliExpress for about 162 USD. As I am not a criminal.

OS Installation

In general in my case it was just following steps from two instructions:

- Using ADB and fastboot
- Install LineageOS on bluepine

In short, what I exactly did, and you should if you choose same phone:

1. Download and extract latest build:
`https://download.lineageos.org/devices/blueline/builds`
2. Download and install USB drivers:
`https://developer.android.com/studio/run/win-usb`
3. Download and extract ADB tools:
`https://dl.google.com/android/repository/platform-tools-latest-windows.zip`
4. Enable developer options on the phone and in developer options enable USB Debugging + OEM Unlock.
 1. Open Settings, and select **About**.
 2. Tap on **Build number** seven times.
 3. Go back, and select System → **Developer options**.
 4. Scroll down, and check the **USB debugging** entry under **Debugging**.
5. Plug phone into computer using USB cable. On the computer, open up a terminal/command prompt in place where you have extracted **adb** binaries and type `.\adb.exe devices`. A dialog should show on your device, asking you to allow USB debugging. Check **always allow**, and press **OK**. If the dialog is not appearing or the list of devices is empty, check if you installed **adb** properly.
 1. If everything works use command `.\adb.exe reboot bootloader`. You can also boot into fastboot mode via a key combination: With the device powered off, hold `Volume Down + Power`.
 2. Once the device is in **fastboot** mode, verify your PC finds it by typing: `.\fastboot.exe devices`
 3. Now type the following command to unlock the bootloader: `.\fastboot.exe flashing unlock` If the device doesn't automatically reboot, reboot it manually. It should now be unlocked.
 4. Since the device resets completely, you will need to re-enable USB debugging to continue. Once you enabled USB debugging reboot it to bootloader again.
 5. Boot a custom recovery using **fastboot**. Flash a recovery on your device by typing (provide path to **boot.img** you downloaded): `.\fastboot.exe flash boot "C:\build\boot.img"`
 6. Now reboot into recovery to verify the installation. Use the menu to navigate to and to select the **Recovery** option.
You should boot to recovery with LineageOS.
 7. Now you can install LineageOS from recovery. Tap **Factory Reset**, then **Format data/factory reset** and continue with the formatting process. This will remove encryption and delete all files stored in the internal storage, as well as format your cache partition (if you have one).

8. Return to the main menu. On the device, select **Apply Update**, then **Apply from ADB** to begin sideload.

On the host machine, sideload the package using: `adb sideload "C:\build\lineage-19.1-20230411-nightly-blue-line-signed.zip"`

9. Once done, click the back arrow in the top left of the screen, then **Reboot system now**.

6. Configure phone after reboot. Suggestions in next step.



System configuration

During the configuration:




- Do not allow apps to use your location.
- Do not send diagnostic info to LineageOS.
- Set 8 digit PIN and add fingerprint if you want (but as you are criminal, better is to setup only strong PIN, it is easier to hit you in the head and use your finger to unlock when you are unconscious than force you to say what the PIN is. At least when you're unconscious, you won't say what is the PIN). Symbols/patterns to unlock phone are also weaker than PIN.
- Set PIN keyboard to be displayed in random pattern so no one will remember the position if peeps over your shoulder.
- Disable sensitive content when locked in **Settings/Notifications**.
- In **Settings** -> **Privacy**, disable camera and microphone access for apps.
- Check if encryption for device is enabled. It should be by the default.
- Disable **USB debugging** in developer options.
- Force each app to be locked by PIN (it's possible in LineageOS protect every app by system PIN or even hide from the menu). Do it even for phone settings.
- Set lockout policy to very short time.
- Disable location, Bluetooth, NFC, turn of camera and mic access


Sat, Apr 15


08:55


Emergency calls only   86%


 


 **Internet** 



 **Location**
Off


 **Bluetooth**
Off

 **NFC**
Off

 **Mic access**
Blocked

 **Camera access**
Blocked

 **Do Not Disturb**
Off

 **Airplane mode**
Off

Root or not to root

I rooted my device, and I control which apps has access to the root. It is not necessary to root, more like optional.

I did these steps to root Pixel 3 with custom LineageOS, may be useful for someone:

1. Enable **USB Debugging**.
2. Download and install latest **Magisk** app.
3. Copy **boot.img** (file downloaded in **OS Installation** step) to the phone memory.
4. Press the **Install** button in the **Magisk card**.
5. Choose **Select and Patch a File** in method, and select the boot image.
6. Start the installation, and copy the patched image to your PC using **ADB**:
`adb pull /sdcard/Download/magisk_patched_[random_strings].img`
7. Flash the patched boot image to your device, reboot into **fastboot** mode and flash with command: `.\fastboot.exe flash boot "magisk_patched_[random_strings].img"`
8. Reboot and launch **Magisk** app, and you will see a prompt asking for environment fix; click and wait for the reboot
9. Disable **USB Debugging**.

To not lost root on each LineageOS update follow these steps:

1. Disable **Automatic system updates** in developer options. So it won't install OTAs without your acknowledgement.
2. Apply OTAs as you normally would (**Settings** → **System** → **System Update**).
3. Wait for the installation to be fully done (both step 1: **installing update**, and step 2: **optimizing your device**, of the OTA), **do not press the Restart now or Reboot button!** Instead, go to (**Magisk app** → **Install** → **Install to Inactive Slot**) to install **Magisk** to the updated slot.
4. After installation is done, press the reboot button in the **Magisk** app. Under-the-hood, the **Magisk** app forces your device to switch to the updated slot, bypassing any possible post-OTA verifications.
5. After reboot news system will be installed and you will still have root.

Apps

Main app you should install is F-Droid. To install other safe and good apps and to keep them up to date. Then using F-droid install other useful apps like:

- InviZible Pro – includes well-known modules such as **DNSCrypt, Tor and Purple I2P**.
- Fennec – web browser based on Firefox with all Firefox options (disable standard web browser from LineageOS)
- If you are fan of Chrome you can choose Bromite. (You need manually add official Bromite repository to F-Droid as it is not available by default)
- OpenKeyChain – for PGP keys
- Keepass2Android – as a password manager
- K-9Mail – mail client
- Tutanota app – mail client as an alternative to other email providers
- Session – communicator
- Monerujo – Monero wallet
- TermBot – SSH client
- OpenVPN Connect – VPN client to connect to own VPN server
- aTalk – jabber client with OTR and OMEMO support
- Aegis – two factor authenticator app.

You should stick to the open-source, stable, long developed apps. Mostly every android app has it own alternative in F-Droid store. You can always look for alternative on website like Privacy Tools, and install apps from the source.

Always verify hash of apps you are installing with hash provided by developer to make sure they were not modified by third party. Before you configure every app, check next step.



This page is also available in the following languages:

English



Go



**Congratulations.
This browser is
configured to use
Tor.**

Your IP address appears to be:

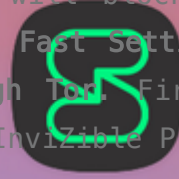
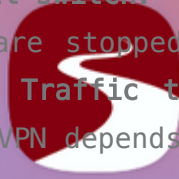
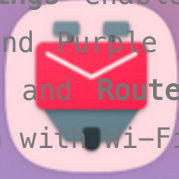
104.244.74.57

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Relay Search](#).



#Torify everything

InviZible Pro is great app allows you to torify all phone network traffic. If you have root use **root mode**, if you decided to not root you phone use VPN mode. In both case in **Common Settings** enable **kill-switch**. This will block internet connection when Tor, DNSCrypt and Purple I2P are stopped. In **Fast Settings** enable DNSCrypt, Tor and I2P on boot and **Route All Traffic through Tor**. Firewall options should allow only connection with Wi-Fi or VPN depends on InviZible Pro mode.



This application combines **Tor**, **DNSCrypt**, **I2P**, **Firewall**, **Kill switch** and many more options.

I tried configure everything by my own using **Orbot** and **AFWall+**, but always something didn't work, or was terminated. Then I found InviZible Pro app and all hours spent on configuration and tutorial I wrote for Orbot and AFWall+ feels useless. Someone already did it correctly and put all in one.

You should go through all option in app and decide what else you want to enable/disable.

I analyzed traffic on the router and I didn't found any connection rather than Tor traffic. I really tried to broke things on the system and app itself, but kill switch always has worked.

In the past I was using standard phone which was connected only to the Tor router. Now thanks to that awesome app I can do the same directly on the phone.



MAIN

DNS

TOR

I2P

- Hide IP with TOR
- Protect DNS with DNSCRYPT
- Access to I2P sites with Purple I2P

STOP

Tor Running

DNSEncrypt Running

I2P Stopped



Internet



Location



Bluetooth



NFC

Silent



InviZible Pro • 18:36:44



TOR & DNSCRYPT

▼ 0 b/s 549.1 MiB ▲ 0 b/s 9.4 MiB

Manage





← Common Settings

Other

Kill switch

Block internet connection when Tor, DNSCrypt and Purple I2P are stopped



Refresh rules

Update rules on every connectivity change



Prevent device sleep

Additional Protection with No Root Mode to prevent app being killed by android. May drain battery



Multi-user support

Support for Dual Apps, MIUI, Island, Shelter and Work profile applications



Help messages

Always Show Help messages



Enable script control

Additional info

Use the following command to manage application modules: "am broadcast -a

pan.alexander.tordnsript.SHELL_SCRIPT_CONTROL --ej dnsdecrypt 1 --ej tor 1 --ej i2p 1

So, in general I have a smartphone connected to the Wi-Fi, where all traffic is routed through Tor. If Tor connection is broken, internet is cut. I am using Riseup and Tutanota as email provider. Riseup allows you to connect and use onion addresses for mail client, so even if there would be issue with configuration, if my traffic won't be torified, I won't be able to connect to the mail server. Tutanota allows to disable IP logging. If you do not trust any email provider you can setup your own mail server, and harden it properly. For communication I choose Session communicators and encrypted emails. Using this configuration I could also install for example Signal app, or some jabber client with OTR orOMEMO support like aTalk.

Select SysBox

Don't forget to choose secure XMPP server. Here are some lists: Jabber.at, Jabberes.org, Jabberworld.info, or if you trust no one, setup your own jabber server only for your criminal organization xD.

I resigned totally from using phone as phone itself, I have no physical number, or sim card, and I can only communicate securely using various channels like apps or emails. It is just pocket PC with access to the Internet. Not a smartphone, but an anonymous mobile privacy smart net device. Yeah smartphone without phone... so just smart xD.

It is going a little bit harder when it comes to have phone number, with internet data package, as for now I am limited to the working Wi-Fi. If I would be traveling and there will be no Wi-Fi I would probably be offline. But that's can be also part of strategy. Do not be online all the time, but only when in safe places. Unfortunately, this also can be a weak point, if some of the location will be compromised, or if someone learns that this is how it works, that when I am in any of my places I am online, and when I travel I am offline. This is why I am adding additional chapter about mobile data.

Mobile data

There are two ways to handle this. Using mobile hotspot on the other device with anonymous sim card, or using anonymous sim card in the mobile phone itself. As I resigned totally from having phone number in this scenario I am happy to use first method.

Another smartphone with sim card bought anonymously, and registered for some fake data, or other person, not related to me. Just as a hotspot, to turn on when needed. Not all countries required personal data during the phone number

registration. Like for example in my county there is a lot of offers from our neighbors Czech Republic, where registration is not required. So sellers in Czech offer activated card and send it to any location you want. You just need to top-up card, from time to time using some anonymously bought top-up cards, or directly by bitcoins on services like this. Czech is just one example. Browse eBay's offers for anonymous or registered sim cards. Thousands of offers. Just choose the best one, which can be top-up easily with some anonymous option or cryptocurrency.

hoek © 2018-2023

[Home](#) | [Post](#) | [Projects](#) | [Search](#) | [Category](#) | [Tag](#) | [Rss](#) | [\\$](#) | [\\$](#)

At the end, all mobile traffic will be used for Tor connection so even if someone would intercept somehow traffic from mobile phone used as hotspot, will see just encrypted data. Also phone number itself will not be related to any criminal activities. It just provide mobile data for other device.

Many operators provide also eSim card, which is very good alternative to standard sim card. As you do not need to have any drop point where card needs to be send, as eSim is virtual, but always double check if your phone supports eSim. For example Pixel 3 have one chip for eSim.

#Mobile number

If you really need a phone number to register some services that require phone number, or for any other reason, use websites like SMS-Activate for virtual numbers, or one time registration. For second number Vyke app is also alternative or Burner. Mentioned earlier eSim solutions is also something to consider. You can always use temporary and anonymous burner phone for specific occasion, and provide your number to other interested people using encrypted chat app. When everything ends, just destroy phone and buy new one.

#OPSEC

All previously described tips are nothing if you will act like a dumbass. Strongest encryption will not protect you if your phone will be left not locked in the public place :) So here are some good practice's.

- Never use your secure phone in not trusted locations, not only strange Wi-Fi, but also physical places.
- Never unlock your phone or enter the pin, if someone is watching your screen.
- Never do anything on the phone when it is possible, that screen of your phone is watched, or monitored by some people, or cameras (metro video monitoring system, city surveillance system etc.)

- TBH never use that phone in public places where there is a lot of people, who can observe you, try to steal your phone, or catch it when it is unlocked.
- Use only encrypted communication channels, and if possible force auto delete messages timer. Delete emails you already read and do not need for later.
- Do not remember passwords in apps and browser, always use password vault, and for each activity copy and paste password from vault.
- Use strong password for password vault.
- Set up 2fa everywhere.
- Backup your mobile phone stuff in secure and encrypted location, in case you have to destroy it and setup new one.
- Destroy phone in case if you are in a trap, its encrypted, no one will get any information from it. But if it will be working, someone always will find a way to force you to provide PIN.
- If possible, setup auto wipe phone if PIN is entered incorrectly 3 times. Setup safe trigger PIN, if someone will enter it, phone will be wiped out. Then if phone is not in your hand you can tell false pin and your opponent will wipe it for you :)
- Always have backup device in safe location in case if first one is destroyed/damaged.
- Remember that mobile phone is just additional device. For quick check stuff and communication close at hand. Your main virtual machine or laptop should be main place for everything.
- Never buy anything in person, or by credit cards related to your real name and identity.
- Never buy any special crafted software for thieves, or offering great anonymity. Use only tested, trusted software and services with good reputation.
- Never leave your phone unattended.
- Make sure you separated all standard apps, accounts, numbers, services from the one you are using as a criminal.
- Never take phone on the action ;)
- If you are using standard sim cards and your phone is related to some numbers and cellular network, have a Faraday Bag to fully cut it off if needed.
- You can also use apps like IMSI catchers to detect unusual/fake cell towers.
- Keep all software and system up to date, use only trusted official repositories.

Here is also interesting book to check: Mobile phone security for activists and agitators.

End notes

A little bit chaotic. But if I would be for example a dark web market owner, and wanted to have possibility quickly contact with coworkers, and customers, I would be able to manage my stuff using smartphone configured in this way. I hope so.

Fortunately I am not a criminal and all that description and configuration was just a test and a lot of fun. Just to check if it is possible to achieve some kind of privacy and anonymity with the smartphone. If another El Chapo would like to have a secure mobile phone, I can configure it for part of the empire and the hand of the daughter, nah just kidding, his daughter was not in my type, and my wife would kill me.

I hope the above tutorial may be useful for some whistleblowers, or people who are in danger somehow and need to keep themselves anonymous, and need to communicate in secure way.

Please add your suggestions in the comments.