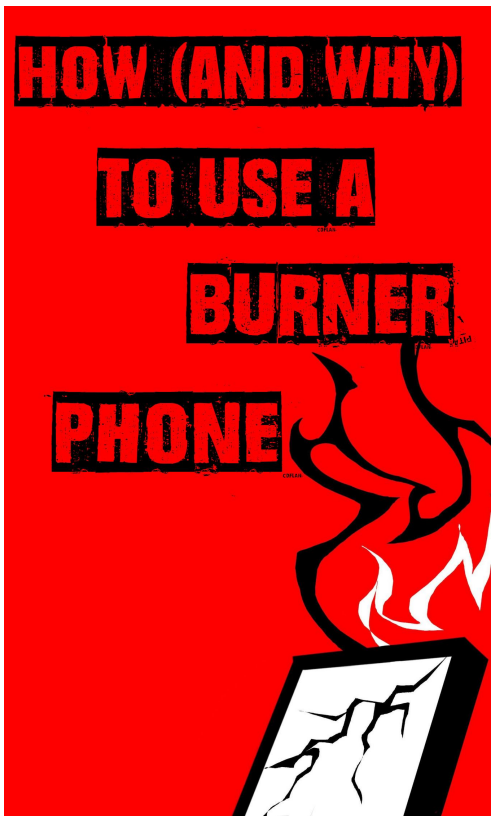
How (and Why) to Use a Burner Phone

Anonymous



11/2/2023

Contents

How (and Why) to Use a Burner Phone

Mobile phones are vital for on-the-ground resistance coordination; however they weren't designed with privacy and security by default. Not only do they do a poor job of protecting your communications, they also expose you to surveillance risks — especially GPS and cellular tower location tracking. As an example, the FBI can submit a warrant to a cellular service provider for the phone numbers and associated information (such as location history from GPS or cellular towers) of cell phones that were close to an event. The radius of search around the event can be several miles and they can use a large time window to search for phone numbers. From this information they can determine what phones were in the area, who those phone numbers regularly communicate with, and any identifying information tied to the phones. To learn more about what the FBI and other law enforcement agencies can do with your cell phone data, and how they obtain it, see the FBI CAST Geo-Location Field Resource Guide in the Additional Reading section. The following guide explains how to set up and use a burner phone to minimize these risks.

A 'burner phone' is a mobile cellular phone purchased with the intention of destroying (burning) it in the near future. Burner phones are inexpensive (usually $20-$40) and purchased in cash along with a prepaid (no contract) plan. A burner phone should have a removable battery and should not be linked to your personal identity and social networks in any way. If a phone is never tied to your personal identity, or the identity of comrades, friends, and family, any metadata or location data captured by law enforcement will tell them little more than that a person was in a location using a mobile phone.

Burning a phone entails first wiping the phone (factory reset), then opening the phone, removing and smashing the sim card, smashing the electronics inside, then lighting the phone, sim card, and electronics on fire and discarding the melted remains in a safe spot, or throwing all components into a safe body of water at least a few feet deep. Be careful to remove the battery before burning it (the battery will explode in fire).

Sometimes a burner phone refers to a mobile cellular device that will be used only one time. This guide describes practices for using a burner phone over a longer period of time. These phones are used in a closed network of burner phones, where neither the burner phones nor their contacts are connected to government names. You should keep a burner phone for no longer than a month, and burn phones more frequently if needed, particularly if the network is compromised, for example if one of the members of the burner network is arrested.

Burner phones should also be used for civilian purposes ("civ phones") because they are not tied to your identity. Civ phones may be tied to other phones that are identifiable (such as friends and family). There are comrades who have used only burner civ phones for decades with no problem; they are just as effective for civilian purposes as contract phones, and are also much cheaper.

Although mobile phones can be made safer, no tool can ever fully protect your privacy. The safest way to protect yourself is to **never discuss any sensitive topics**, **never record any sensitive information**, and **never use a phone to communicate sensitive information**. Law enforcement cannot use evidence that does not exist. A good idea is to imagine the consequences if your phone were to be confiscated and your messages and contact list were to be read aloud in a court of law.

If you must communicate sensitive information, always do it on a **need-to-know basis** (compartmentalization) using **coded language**. Compartmentalizing information to only the individ-

uals who need to know limits the potential for information leak to law enforcement, and using coded language prevents law enforcement from understanding any information that is leaked.

Not generating sensitive information, compartmentalizing, and using coded language are the three most important tactics to protect your communications from law enforcement. Practice them. Use them. Be strict.

DO's and DONT's for using a burner phone

- DO purchase your burner phone and plan with cash

  It is preferable to purchase the phone from a location away from where you live, using cash and protecting your identity as much as possible (e.g., buying with a hat and face mask). Cover anything identifiable (hair, piercings, tattoos). Even better, have a trusted comrade buy it with cash.

  Leave your civ phone at home while purchasing and activating the burner phone.

- DO activate the phone away from home on a public network

  Options include public libraries, McDonalds, or anywhere with public WiFi.

  Avoid surveillance cameras when buying and activating the phone.

  Once the phone is activated, destroy any packaging that contains the IMEI, SIM numbers, and data plan info.

- DO create a phone number with a non-identifying area code

  Most pre-paid plans allow you to choose the zip code the new phone number will originate from. Some strategies include using a random zip code generator, or using a zip code that's different than where the phone will be used but has the same area code.

- DO create a brand new Gmail account for your phone and account activation

  (For Android phones): Creating a Gmail account is not strictly necessary; however you will not have access to the Play Store without one.

  Use a username for the account that is unrelated to any of your other accounts or identities. Do not try to be clever; randomness is always better than cleverness.

- DO use a VPN if you need to browse the internet

  RiseupVPN is the bare minimum. It is free, easy to install, and should always be turned on. There are VPN settings in the phone ("always-on VPN" and "block non-VPN traffic") that prevent connections without a VPN.

  ProtonVPN works well and is free but requires you to create a protonmail account. You can do this without supplying any identifying information.

  Mullvad or iVPN are good paid options. They can paid for using crypto-currency.

- DO use private browsing and search

Use Firefox instead of Chrome. Firefox has an "always-private" browsing option (and other options you can set to enhance privacy). DuckDuckGo is a relatively private search option (though there may be better options).

See Appendix A below for Firefox settings.

- DO use Signal

  Install and use the Signal app immediately for all text and voice calls.

  Signal provides end-to-end encryption which prevents law enforcement from decoding your communications when intercepted. However it does contain metadata about who you've messaged and when, so be mindful of who you message and how you store their information in your phone.

  See Appendix B below for Signal settings.

- DO go through your burner phone settings carefully and make sure they are set to the most secure options

  There are many settings on your burner phone that you should make as strict as possible. Familiarize yourself with them.

  See Appendix C below for phone settings.

- DO remove bloatware

  Once connected to a VPN, the phone might automatically install bloatware. Remove these apps, and keep in mind that the more apps on the phone, the more metadata are generated. Remove as many apps as possible.

- DO use coded language around your phone

  Develop coded language with your comrades and always use it.

  Use code-names for each other. Change code-names periodically. NEVER associate code-names and government names, or code-names and Signal names.

- DO turn off your burner and remove the battery when having sensitive conversations

  Sensitive information should never be discussed near phones, even if they are turned off. The battery must be removed. If you cannot remove the battery, store the phone in a safe nearby location that cannot hear you.

  Never have sensitive conversations inside or near buildings or other commonly used spots.

- DON'T bring phones to actions unless they are needed

  Never bring a civ phone to an action.

  Avoid bringing burner phone if you can. Leave no traces (physical or cyber).

  When considering bringing burner to action: Think about what would happen if the cops got the phone and whether bringing the phone is worth the risk. To minimize risk, delete as much as possible before bringing burner to an action.

- DON'T link any burner phones in the closed network with civ phones, either in physical proximity, or through digital contact

  Don't turn on the burner phone near your civ phone or the civ phone of your family, friends, and comrades.

  Having two phones in the same location creates metadata that links the two devices. Ideally you will not have your burner phone near civ phones, even when it's off.

- DON'T log into personal accounts on your burner phone

  Once personally-identifying info is tied to a device it is trivial for law enforcement to locate you if they want to.

- DON'T message your civ friends on the burner

  Metadata about your social networks (which is generated even by Signal) can identify you.

- DON'T message your former contacts with your old name and number

  Create a passcode or phrase together, ideally in person, that will inform the person you're contacting who you are.

- DON'T invite yourself to groups with your old burner

  Connecting new and old burners (or civ phones) in any way defeats the purpose of burning the phone, which is to break all connections that may have been established on the old phone.

Example: Setting up a Straight Talk TCL A3 phone

Here is an example of setting up a Straight Talk TCL A3 phone to be a burner phone. This can be purchased from Walmart. The other Straight Talk phones from Walmart will have a similar setup. Be sure to get a phone with a removable battery.

- Purchase the phone

  Do not bring your phone or any identifying information into the store (usually Walmart). It is better to ride a bike or walk to the store, but if you must drive be sure to park far away enough that your license plates cannot be read, and then walk the rest of the way. Use a hat and face covering in the store. Pay in cash. Do not buy anything else in the store. Do not bring any other phones or electronic devices. Buy the bronze plan (10gb high speed with 5gb hotspot) or silver plan (unlimited high speed with 5gb hotspot).

- Leave the store and walk to a location with public WiFi

  Stay masked up with hat on. Avoid cameras and people. Use the WiFi. Be mindful of street cameras.

- Open the phone and connect

  Open the phone box, take out the phone, put battery in, and find the red activation card. The red activation card is all you need in addition to the data plan code; throw everything

else away, and be sure to throw the red activation card and data plan card away (or better burn them and throw the ashes away) when activation is complete.

- Turn off all the bad settings

  Go through your settings carefully to look for ones that compromise security (e.g., needlessly storing or transmitting data) or that you simply don't want; for example:

  settings > sound and vibration > silent mode on

  settings > sound and vibration > more sound settings > vibrate on touch off

- Activate the phone

  Go to https://straighttalk.com/activate. Click on the activate button. Wait, wait, wait, try not to hurl the phone if it hangs. The website sucks. Click 'ask for new number'. Generate a random zip code from randomzipcode.com. Then put in the IMEI which is the top number on the red card that came with the A3 device. Select use physical sim card. Input the data plan number by scratching off the back of the card. Input random Gmail and password to finalize account.

- Install RiseupVPN

  Download riseupVPN. Turn it on. Go to settings. Search the word "VPN". Click on VPN, then VPN settings gear button. Click the VPN "always-on" option and "block non-vpn connections".

- Install Signal

  Download Signal, follow the setup information, set disappearing messages to 8hr (or less, depending on the risk), etc.

- Install Firefox

  Download Firefox. Set up always private link. Set default search to DuckDuckGo or other private search.

- Delete bloatware

- Finish setup

  Turn off phone and remove battery. Only put battery back in and turn on when away from other civ phones.

- Follow DOs and DON'Ts and security culture practices above

Afterword

So far physical security is a much bigger risk than phone security when this guide is followed. You're much more likely to get physically nabbed, caught on camera, or snitched on than having some problem with your phone. For this reason burners are just a tiny piece of security culture. Take your physical security very seriously.

More Reading

https://theanarchistlibrary.org/library/crimethinc-what-is-security-culture
https://ssd.eff.org/en/playlist/privacy-breakdown-mobile-phones
https://www.eff.org/deeplinks/2022/10/california-court-suppresses-evidence-overbroad-
https://www.documentcloud.org/documents/21088576-march-2019-fbi-cast-cellular-analysi

Appendix A: Firefox Settings

Open Firefox. Go to the top right and find the three vertical dots and click them. This should bring up the menu. Click Settings near the bottom of the menu.

Search

- Select DuckDuckGo or other private search engine
- Turn off all address bar settings
- Set to close after 1 day. Do NOT leave dozens of tabs containing criminal conspiracy evidence open.

Homepage

- Turn of all settings

Logins and passwords

- Turn of all

Autofill

- Turn off all

Set as default browser

- Turn on

Private Browsing

- Click “add private browsing shortcut”. Remove the regular Firefox shortcut and always use the private browsing shortcut.
- Turn on “open links in a private tab”
- Turn off “Allow screenshots in private browsing”

HTTPS-Only Mode

- Turn on

Enhanced Tracking Protection

- Turn on

Site Permissions

- Turn off all

Delete browsing data on quit

- Turn on

Notifications

- Turn off all Firefox notifications

Data Collection

- Turn off all

Advanced

- Turn off all

Appendix B: Signal Settings

Profile

- Create a pseudonym for your account. This should not be linkable to you in any way.

Account

- Use PIN reminders.
- Enable Registration Lock so your number can't be used again without a pin, and make sure to set it to automatically relock after a short period of time.

Chats

- Turn off: Generate Link Previews, Use Address Book Photos, Use System Emoji, Enter Key Sends.
- Disable Chat Backups.

Stories

- Turn off Stories.

Notifications

- Turn off all notifications (You will have to check signal to see whether you have received messages. That is good. You don't want your phone vibrating while you're hiding in bushes 3 feet from cops).
- At a minumum, disable messages from being shown in notifications. Ideally, disable names also.

Privacy

- Turn off Read Receipts and Typing Indicators.
- Enable a default timer for chats, ideally 8 hours. No longer than 1 day. During intense action, 30 minutes.
- Make sure Signal has a Screen Lock.
- Turn on Screen Security and Incognito Keyboard.

Advanced

- Turn on Always Relay Calls.

Appendix C: Phone Settings

Network & Internet

- Turn off: Hotspot \& Tethering, Data Saver.
- Turn on VPN: Select your VPN and use "Always-on VPN" and "Block connections without VPN".
- Set Private DNS to Automatic.

Connected Devices

- Turn off Bluetooth and WiFi.

Notifications

- Turn off Notification History.
- Turn off all Notifications.
- Notifications on Lock Screen: Set to "Don't show any notifications".
- Turn off wireless emergency alerts.
- Turn off enhanced notifications.
- Turn on notification dot on app icon.

Battery

- Turn on Battery Saver, Adaptive Battery, Optimized charging, Overcharge protection.
- Turn on Battery Percentage: Show battery percentage in status bar.

Sounds & Vibration

- Turn off everything.

Display

- Lock screen: Don't show notifications at all.
- Screen timeout: After 30 minutes of inactivity.
- Appearance: Dark Theme.

Security

- Find My Device: Location is off.
- Screen Lock: Choose a PIN, pattern, or password. If you use a swipe pattern be sure to disable the visible pattern and automatically lock.
- Do NOT use Fingerprint or Face Unluck.
- Do NOT use Smart Lock.
- Encryption & Credentials: Make sure your device is encrypted.

Privacy

- Permission manager: Turn off all permissions.
- Turn off: Microphone access, show passwords.
- Notifications on Lock Screen: Don't show notifications at all.
- Android System Intelligence: Turn off.
- Turn off: Show clipboard access, autofill services from Google, Google location history.
- Remove notifications from lock screen.
- If you have a Google account, make sure it's a burner account that has no connection to your identity, and disable Google location history and any other saved info.
- Turn off usage and diagnostics.

Location

- Set Use Location to off. (Note: this does NOT prevent your location data from being tracked — any cell phone is constantly communicating with cell towers and WiFi networks.)

Safety & Emergency

- Turn off all settings.

Passwords & Accounts

- Turn off automatically sync app data.

Google

- Turn off Find My Device.
- Personalize using shared data: Turn off all.

System

- Under Languages & Input > Virtual Keyboard > Gboard > Advanced: disable usage statistics, personalization, and improve voice and typing for everyone.

Anonymous
How (and Why) to Use a Burner Phone
11/2/2023

https://berkmananarchy.noblogs.org/post/2023/11/02/zine-submission-how-and-why-to-use-a-burner-phone/

usa.anarchistlibraries.net