Elle Armageddon
Burner Phone Best Practices
A User's Guide
March 27, 2017

Retrieved on 29th October 2020 from crimethinc.com

usa.anarchistlibraries.net

Burner Phone Best Practices

A User's Guide

Elle Armageddon

March 27, 2017

Contents

Burner phones are not the same as disposable phones. . . 5
Burner phones should only ever talk to other burner phones. 5
Never turn your burner on at home. 6
Never turn your burner on in proximity to your main phone. 6
Don't refer to yourself or any of your contacts by name. . 6
Beware of IMSI catchers. 7
Burner phones are single-use. 8
Procure your burner phone carefully. 8
Never assume burner phones are "safe" or "secure." . . . 8

that someone is likely to be careless. This is another good reason to be careful with your communications even while using burner phones. Always take responsibility for your own safety, and don't hesitate to erase and ditch your burner when necessary.

Burner phones are single-use.

Burner phones are meant to be used once, and then considered "burned." There are a lot of reasons for this, but the primary reason is that you don't want your clandestine actions linked. If the same "burner" phone starts showing up at the same events, people investigating those events have a broader set of data to build profiles from. What this means is, if what you're doing really does require a burner phone, then what you're doing requires a fresh, clean burner every single time. Don't let sloppy execution of security measures negate all your efforts.

Procure your burner phone carefully.

You want your burner to be untraceable. That means you should pay for it in cash; don't use your debit card. Ask yourself: are there surveillance cameras in or around the place you are buying it? Don't bring your personal phone to the location where you buy your burner. Consider walking or biking to the place you're purchasing your burner; covering easily-identifiable features with clothing or makeup; and not purchasing a burner at a location you frequent regularly enough that the staff recognize you.

Never assume burner phones are "safe" or "secure."

For burner phones to preserve your privacy, everyone involved in the communication circle has to maintain good security culture. Safe use of burners demands proper precautions and good hygiene from everyone in the network: a failure by one person can compromise everyone. Consequently, it is important both to make sure everyone you're communicating with is on the same page regarding the safe and proper use of burner phones, and also to assume

A burner phone is a single-use phone, unattached to your identity, which can theoretically be used to communicate anonymously in situations where communications may be monitored. Whether or not using a burner phone is itself a "best practice" is up for debate, but if you've made the choice to use one, there are several things you should keep in mind.

Burner phones are not the same as disposable phones.

A burner phone is, as mentioned above, a single-use phone procured specifically for anonymous communications. It is considered a means of clandestine communication, and its efficacy is predicated on having flawless security practices. A disposable phone is one you purchase and use normally with the understanding that it may be lost or broken.

Burner phones should only ever talk to other burner phones.

Using a burner phone to talk to someone's everyday phone leaves a trail between you and your contact. For the safety of everyone within your communication circle, burner phones should only be used to contact other burner phones, so your relationships will not compromise your security. There are a number of ways to arrange this, but the best is probably to memorize your own number and share it in person with whoever you're hoping to communicate with. Agree in advance on an innocuous text they will send you, so that when you power your phone on you can identify them based on the message they've sent and nothing else. In situations where you are meeting people in a large crowd, it is probably OK to complete this process with your phone turned on, as well. In either case,

it is unnecessary to reply to the initiation message unless you have important information to impart. Remember too that you should keep your contacts and your communications as sparse as possible, in order to minimize potential risks to your security.

Never turn your burner on at home.

Since cell phones both log and transmit location data, you should never turn on a burner phone somewhere you can be linked to. This obviously covers your home, but should also extend to your place of work, your school, your gym, and anywhere else you frequently visit.

Never turn your burner on in proximity to your main phone.

As explained above, phones are basically tracking devices with additional cool functions and features. Because of this, you should never turn on a burner in proximity to your "real" phone. Having a data trail placing your ostensibly anonymous burner in the same place at the same time as your personally-identifying phone is an excellent way to get identified. This also means that unless you're in a large crowd, you shouldn't power your burner phone on in proximity to your contacts' powered-up burners.

Don't refer to yourself or any of your contacts by name.

Given that the purpose of using a burner phone is to preserve your anonymity and the anonymity and the people around you, identifying yourself or your contacts by name undermines that goal. Don't use anyone's legal name when communicating via burner,

and don't use pseudonyms that you have used elsewhere either. If you must use identifiers, they should be unique, established in advance, and not reused.

Consider using an innocuous passphrase to communicate, rather than using names at all. Think "hey, do you want to get brunch Tuesday?" rather than "hey, this is Secret Squirrel." This also allows for call-and-response as authentication. For example, you'll know the contact you're intending to reach is the correct contact if they respond to your brunch invitation with, "sure, let me check my calendar and get back to you." Additionally, this authentication practice allows for the use of a duress code, "I can't make it to brunch, I've got a yoga class conflict," which can be used if the person you're trying to coordinate with has run into trouble.

Beware of IMSI catchers.

One reason you want to keep your authentication and duress phrases as innocuous as possible is because law enforcement agencies around the world are increasingly using IMSI catchers, also known as "Stingrays" or "Cell Site Simulators" to capture text messages and phone calls within their range. These devices pretend to be cell towers, intercept and log your communications, and then pass them on to real cell towers so your intended contacts also receive them. Because of this, you probably don't want to use your burner to text things like, "Hey are you at the protest?" or "Yo, did you bring the Molotovs?"

Under normal circumstances, the use of encrypted messengers such as Signal can circumvent the use of Stingrays fairly effectively, but as burner phones do not typically have the capability for encrypted messaging (unless you're buying burner smartphones), it is necessary to be careful about what you're saying.