Cyber resilience guide

Version 0.1 (2022)

Reddit: @sec4all

GUIDE

Most apps are hosted on Fdroid, an open source alternative of PlayStore. You can find alternatives, just make sure they're reviewed by trustworthy sources.

Communications

When the Internet goes out

In the case you are unable to chat over the Internet, I would recommend one option to communicate in real time:

- Briar : https://briarproject.org/download-briar/

Decentralized, Briar use TOR while on WI-FI mode, which brings a big security layer, and most importantly here, it **can work on BLUETOOTH** for short range distances.

To add a contact on Briar, you must both add each other first. You can either exchange briar ID links or scan a contact’s QR code if they are nearby.

There's the option for group chats, audio and video calls.

It only works on ANDROID, and **all parties need to be online to exchange messages (no offline mode as there are no servers directly involved)**

Be aware that the adversary must have limited ability to monitor short-range communication channels for Briar to be considered, as stated here: https://briarproject.org/how-it-works/

And the manual to begin with: https://briarproject.org/manual/

SMS

The case of SMS is tricky, but is the main choice for most of us. The fact is, GSM networks weren't designed with privacy and security in mind, so be aware of multiple vulnerabilities.

- SIM card tracking (ICCID),
- IMEI tracking (serial number),
- SMS (unencrypted),
- IMSI tracking (catchers & stingrays),
- MSISDN tracking (cell number)

...

In short, your messages and calls can EASILY be intercepted, and your position can be compromised in a matter of minutes (unless you're on a public space with a lot of SIM cards around).

The goal is to lower your exposure to these tracking methods, by reducing the amount of data you emit:

- Check these countermeasures from another Redditor. They can be very restrictive, but they show how bad it can be.

Unfortunately, mitigating is not easy for SMS and calls.

Other connections

Common myth debunked:

- Airplane mode disables most of the device's radios (carrier signal, Bluetooth, Wi-Fi) but **not NFC or GPS.**

In a critical situation, you should unplug your SIM card, and be aware that your smartphone pings directly from hardware parts, so it can't be 100% safe.

Most often:

- **turn off location**,
- **disable "Turn on Wifi automatically"** to prevent pings,
- **disconnect Bluetooth**.

Online messaging

Think End to End encryption (E2EE) first, meaning the servers can't decrypt and see your communications. Most apps don't include E2EE, while some use their own encryption, which are not widely reviewed by the community.

That's the case for **Telegram**, a lot of factors such as bots attacks and metadata leaking makes it a less safe option, you should avoid it if possible.

- Signal: https://signal.org/ Well known, good security features (sealed sender, PIN code locking...), messages and audio/video calls are End to End encrypted.

Inspecting and Hardening your smartphone

Some tools help you monitor networks and requests passing by your smartphone.

- PilferShush Jammer: https://f-droid.org/en/packages/cityfreqs.com.pilfershushjammer/ Passive and active microphone jammer,
- SnoopSnitch: https://f-droid.org/en/packages/de.srlabs.snoopsnitch/ Monitor for possible IMSI tower nearby,
- Pcapdroid: https://github.com/emanuele-f/PCAPdroid Examine the connections made by user and system apps,
- Blokada: https://blokada.org/#download More user friendly than Pcapdroid, does pretty much the same,

- Ooni: https://ooni.org/install/mobile Monitor network for censorship (not a discreet process, be careful).

Finally, be aware about what you install, a lot of apps are not monitored and contains malware to spy on your communications.

For medium/advanced users, you could even compare the hash of the app with the expected one from the website:

- Deadhash: https://codedead.com/software/deadhash/

Panic button

A tool that brings a panic button for your smartphone, and when triggered, it could delete some apps and files you judge too sensitive.

- Ripple: https://guardianproject.info/apps/info.guardianproject.ripple/

Physical security

If you leave a place, and want to make sure nobody's snooping around, Haven can monitor microphone audio and camera video directly from a smartphone, and send the alert to a phone number and/or device.

- Haven: https://guardianproject.info/apps/org.havenapp.main/

Encrypting data

You might have sensitive data such as governmental documents you need to keep secure. Some apps let you create an encrypted volume directly on your smartphone.

- Droidfs: https://f-droid.org/en/packages/sushi.hardcore.droidfs/ sets up encrypted volumes managed by passwords.

For computers: https://www.veracrypt.fr

Store those passwords in a password manager !

Virtual machine

If you have doubts about your computer being infected, or want to open a file in a more restricted place, you can run a virtual machine to test it.

- Virtualbox: https://www.virtualbox.org/ (see the part "Phishing and URL" for more tools).

VPN

While using Wi-Fi or cellular network, your Internet Service Provider can snoop on the traffic, or the router/public Wi-Fi can be compromised.

That's where a VPN is useful (in addition to the possibility of accessing blocked content through the provider's DNS).

Attention, some of them have tight links with questionable companies, the ones I put are just "safe" enough from now, things can evolve quickly.

Check if your connection is not leaking: https://www.dnsleaktest.com

Accounts needed

- ProtonVPN: https://protonvpn.com/
- Windscribe: https://windscribe.com/download

No accounts (both are well known as privacy defenders)

- RiseupVPN: https://f-droid.org/en/packages/se.leap.riseupvpn/
- CalyxVPN: https://f-droid.org/en/packages/org.calyxinstitute.vpn/

TOR (Orbot)

Orbot proxies your traffic thru the TOR network, and can be an alternative to a VPN.

- Orbot: https://guardianproject.info/apps/org.torproject.android/

HUMAN SIDE

Be careful about what you post online. Every data is sensitive, even the ones you don't suspect.

Delete metadata from pictures on Android:

- Scrambledeggsif: https://f-droid.org/en/packages/com.jarsilio.android.scrambledeggsif/

Phishing and URL

Test an URL:

- https://urlscan.io

Test a file, hash:

- https://virustotal.com
- https://www.joesandbox.com

Other good links

An incredible resource for security and privacy: https://anonymousplanet.org/guide.html

More private and secure tools: https://privacyguides.org

This guide from EFF for protesting resume the precautionary measures when in a sensitive palace: https://ssd.eff.org/en/module/attending-protest

---