OPSEC
operational security

Aktions Handy

Generell gilt:

- keine echten Namen angeben
- billig Tastenhandys verwenden

Um nicht sofort als Aktionshandy aufzufallen, solltest du:

- fake Kontakte einspeichern
- SMS an irgendwelche Nummern schicken

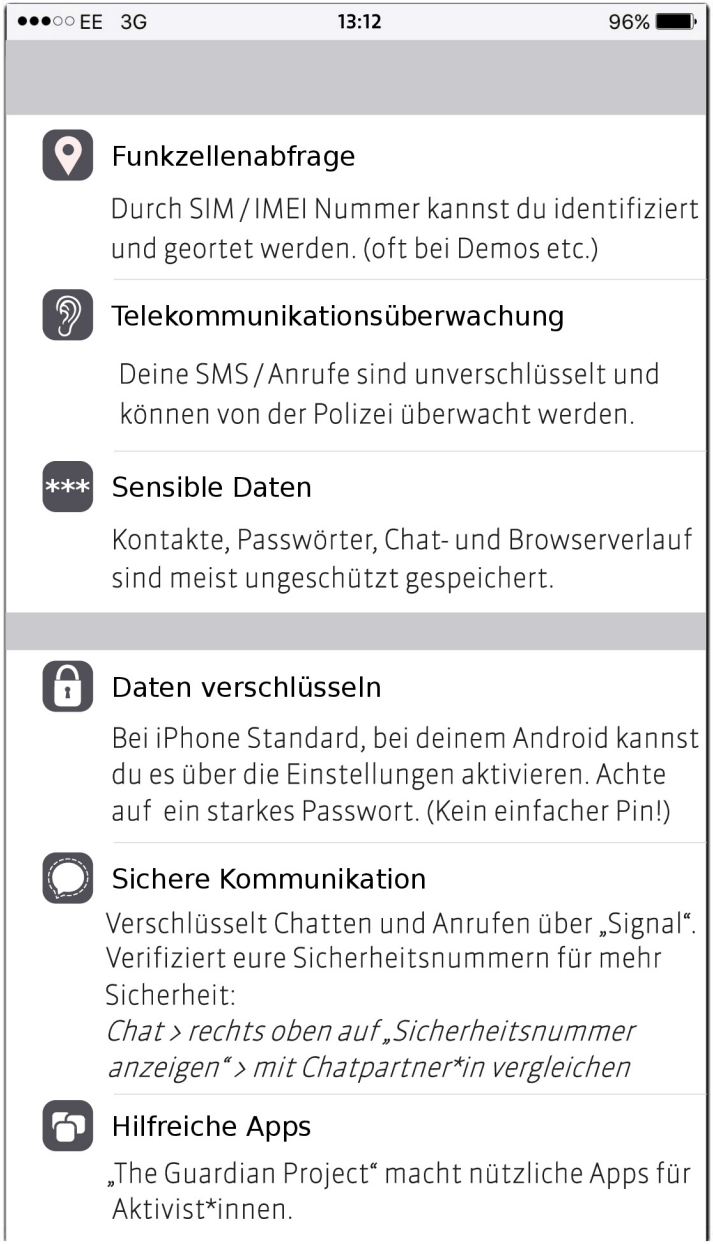
Das sind häufige Fehler:

- Co-Acitivity (Aktions und Privates Handy gleichzeitig an.)
- Co-Localize (Aktions und Privates Handy am selben Ort an.)
- Co-Contact (Kontakte vom Privaten Handy sind auch im Aktionshandy.)
- Real Data (Echte Infos auf dem Aktionshandy gespeichert.)
- Match entry/exit (Aktionshandy geht direkt online sobald das Private Handy aus ist. Und umgekehrt.)

Loswerden:

Nach einer Aktion solltest du dein Handy am besten loswerden. Tipp: Lass es an und kleb es unter einen LKW oder leg es in einen Abfalleimer im Zug. Dadurch kommt es weit weg vom Aktionsort und simuliert dabei noch ein Fake Bewegungsprofil.

Smartphone?


●●●○○ EE 3G
13:12
96%
Funkzellenabfrage
Durch SIM / IMEI Nummer kannst du identifiziert und geortet werden. (oft bei Demos etc.)
Telekommunikationsüberwachung
Deine SMS / Anrufe sind unverschlüsselt und können von der Polizei überwacht werden.
***
Sensible Daten
Kontakte, Passwörter, Chat- und Browserverlauf sind meist ungeschützt gespeichert.
Daten verschlüsseln
Bei iPhone Standard, bei deinem Android kannst du es über die Einstellungen aktivieren. Achte auf ein starkes Passwort. (Kein einfacher Pin!)
Sichere Kommunikation
Verschlüsselt Chatten und Anrufen über „Signal“. Verifiziert eure Sicherheitsnummern für mehr Sicherheit:
*Chat > rechts oben auf „Sicherheitsnummer anzeigen“ > mit Chatpartner*in vergleichen*
Hilfreiche Apps
„The Guardian Project“ macht nützliche Apps für Aktivist*innen.