Ghid de supraviețuire digitală

Anonim

2021

Cuprins

Ghid de supraviețuire digitală

sfaturi și reflecții cu privire la utilizarea instrumentelor digitale între activiști

part. I

Broșura aceasta este o traducere liberă a unui text scris în franceză de niște compa de la Zad du Carnet în 2020/2021. Zad du Carnet a fost o zona de luptă ocupată împotriva distrugerii a 110 hectare de arie naturală pentru un proiect industrial. Această ocupație a fost evacuata în martie 2021, însă lupta continuă. Traducerea aceasta este un tribut adus acestei lupte și un gest care își propune să facă gândurile anarhiste să călătorească dincolo de granițe.

Această broșură este traducerea primei părți a textului original. O traducere a celei de-a doua părți este în curs de desfășurare. În plus, este important de menționat că contextul activismului și a supravegherii în Franța diferă foarte mult de cel din România. Prin urmare, trebuie depuse eforturi importante pentru a adapta anumite puncte a acestei broșuri la realitățile românești. Toate remarcile și comentariile sunt binevenite.

Ne puteți scrie la următoarea adresă :
supravieturedigitala@riseup.net

În această traducere, am încercat să degender textul (așa cum a fost făcut și în textul original), folosind scrierea inclusivă. Aceste forme, dacă uneori fac lectura mai laborioasă, au însa meritul de a ne face să reflectăm asupra colonizării limbii de către patriarhat.

Diversitatea tacticilor există și în protecția digitală.

Folosirea uneltelor digitale nu este un gest inofensiv. A nu lăsa urme și dovezi pe telefon sau pe calculator este o misiune imposibilă. Utilizarea smartphone-urilor și a calculatoarelor fiind conștienți de condițiile de lucru deplorabile din industria care produce aceste obiecte, este în sine un act de negare a valorilor noastre anticapitaliste.

Cu toate acestea, internetul și lumea digitală sunt spații de luptă importante și ar fi greșit să nu le considerăm ca atare. A lupta pentru a ne libera de dependența noastră de obiectele digitale în timp ce învațăm să le manipulăm mai eficient în luptele noastre poate părea incoerent. Dar este unul dintre aspectele diversității tacticilor de lupta. Este important să ne înțelegem, să ne tolerăm și să ne ajutăm reciproc între cei care au ales să folosească cât mai putin obiectele digitale și cei care au făcut din internet spațiul lor principal de luptă.

În plus, în contextul activismului, neglijența unora îi poate costa scump pe ceilalți. Și într-un protest, și în timpul unei petreceri într-un spațiu de activiști, fotografiile făcute cu smartphone-ul personal pot fi un ajutor prețios pentru serviciile de informații. În ultimii ani, statele au demonstrat capacitatea lor de a folosi supravegherea digitală ca instrument pentru intimidarea activiștilor[1]. Ideea acestui ghid este

[1] Chiar și, de exemplu, cazul din 8 decembrie 2020, din Franța: activiști sunt arestați pe întreg teritoriul Franței pe baza unor suspiciuni bazate în mare parte pe interceptări telefonice și spionaj digital: `https://soutienauxinculpeesdu8decembre.noblogs.org/`

și de a participa la construcția unei "culturi de siguranță" care să poată permite tuturor să acționeze la nivelul de conflict și de ilegalitate pe care îl doresc[2].

Ghidul acesta este destinat persoanelor care folosesc uneltele digitale ca parte a activității lor activiste. Vom parcurge anumite amenințări (pericole, atacuri posibile) în domeniul digital și vom propune măsuri parțiale pentru a le evita.

Dar este important să ținem minte că securitatea digitală este o chestiune de resurse disponibile. Atacatorii cu timp și bani vor fi mereu capabili să spargă protecția noastră. Măsurile prezentate în ghid nu pot fi niciodată perfecte.

Planul Documentului

Vom vorbi în acest ghid despre atacuri care caută să obțină date digitale pe care am dori să le păstrăm private. Vom prezenta mai întîi cele mai frecvente atacuri, cele legate de erorile omenesti. Vom vorbi apoi despre atacurile specifice telefoanelor mobile. În a doua broșură vom vorbi despre atacuri specifice asupra computerelor și în special cele legate de navigarea pe web.

Este de la sine înțeles că atunci cand folosești un telefon mobil pentru a consulta Signal, poți să fi supus atacurilor specifice telefonului, precum și atacurilor specifice Signal.

Pentru fiecare atac, vom prezenta metode de a te proteja. Aceste metode nu pot fi însă de încredere totală, dar pot îmbunătăți apărarea împotriva unui atacator. Aplicarea unei măsuri de protecție digitală într-un mod eficient înseamnă să înțelegi cum te poate proteja împotriva unui anumit atac, dar și care sunt limitele împotriva altor tipuri de atacuri.

Cu aceste măsuri de protecție, dorim să complicăm spionajul, să evităm recuperarea de date în cazul percheziților și să evităm furnizarea de probe judiciare. Scopul anonimatului total ar fi mult prea ambițios. Această broșură este doar un ghid de supraviețuire și prezintă doar câteva potențiale atacuri și unele măsuri de protecție dar este departe de a fi exhaustiv.

[2] Cultura siguranței este o problemă mai amplă care cuprinde temele abordate în această broșură. Puteți găsi baze de reflecție în următoarele texte: https://infokiosques.net/spip.php?article556 în franceză; Recipes For Disaster : An Anarchist Cookbook pe AnarchistLibrary, în engleză.

1. Atacuri cauzate de erori umane

Erorile umane sunt cauza principală a atacurilor reușite.

1.1 Shoulder surfing

Vorbim despre shoulder surfing când cineva se uită peste umărul altcuiva în momentul în care această persoană folosește un device. Poate să recupereze o parolă, o adresă mail sau niște informații despre un document la care lucrează. Vorbim și de shoulder surfing cînd o cameră de filmat poate să vadă ecranul nostru sau tastatura noastră.

Pentru a ne proteja, putem să fim atenți la camere, să scriem parolele în mod discret fară să ne fie teamă de a fi percepuți ca paranoici, sau mai simplu, să ne punem într-un colț al camerei cînd folosim calculatorul sau telefonul.

1.2 Social engineering

Vorbim despre social engineering cînd ni se extrag informații care am vrea să rămână confidențiale prin manipulări psihologice. De exemplu prin întrebări aparent inocente sau prin simularea un pretext urgent pentru a cere o informație personală.

Metoda de protecție în fața social engineering este atât colectivă cât și individuală. Putem învăța să nu fim curioși și să nu punem întrebări indiscrete.

Pentru a ajuta oamenii să îndrăznească să nu răspundă la întrebări indiscrete, poate fi formalizat, într-un grup, că nu vor fi consecințe sociale negative în cazul unui astfel de refuz.

1.3 Gestionarea slabă a parolelor

Pericole : refolosirea aceleiași parole și parole scurte.

Cu cât o parolă este folosită mai mult, cu atât securitatea ei este mai slabă. Într-adevăr, când folosești o parolă pe o aplicație sau pe un site, nu poți să fi sigurx că acestea stochează în mod sigur parola ta. Dacă oamenii cărora le-ai dat parola sunt atacați, atacatorii pot să recupereze parola și identitatea ta și să le încerce în alte servicii unde ai aceeași parola. Furturile de date sunt foarte comune și puțin mediatizate și este foarte probabil ca combinația ta de ID și parola să se fi scurs deja pe web[3].

O altă eroare sunt parolele prea slabe. Siguranța unei parole depinde de diverși parametrii ca de exemplu lungimea, folosirea caracterelor speciale (majuscule, cifre etc.) și caracterul său aleator. Cele mai bune parole sunt cele generate în mod aleatoriu cu cel puțin 16 caractere. Gestionarul de parole propune această funcționalitate (vezi mai jos). O altă metodă ușoară pentru a-ți aminti o parola robustă este a avea o propoziție simplă, ca de exemplu «Girafele iubesc morcovii roz». Deci parola poate fi «G1r@fel3IubescMorcov11Roz», 25 de caratctere, super robust. Însă acest tip de parolă, cu cuvinte din dicționar, este mai puțin sigură ca parolele aleatorii cu lungime similară.

Password Manager-urile îți fac viața mai ușoară.

Pentru a evita utilizarea acelorași parole de mai multe ori și pentru a avea parole lungi, vă sfătuim să folosți password manager și parole unice.

KeepassXC este un password manager. Acest software poate stoca un număr mare de parole într-o bază de date. Parola pentru a debloca această bază de date trebuie să fie lungă și unică. Acest lucru face posibil să nu trebuiască să îți amintești toate parolele unice pe care le utilizați ci doar pe cea a bazei de date.

[3] Situl Have I Been Pwned identifică scurgeri de securitate și îți spune dacă o parolă legată de adresa ta de mail s-a scurs în timpul unui atac : https://haveibeenpwned.com/

Temps nécessaire à un hacker pour trouver votre mot de passe

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Timpul necesar pentru ca un hacker să găsească parola ta
Surse : Howsecureismypassword.net.

Acestă diagramă ne da o idee de timpul necesar pentru a găsi o parolă cu atac prin forță brută. Datele au deja câțiva ani.

După cum vezi aici, este important să combini cifrele și literele pentru a avea o parolă greu de găsit. Este in special valabil pentru codurile de deblocare a telefoanelor. Atunci când este posibil, opteaza pentru o parola cu litere, e mai buna ca cea care are doar cifre.

1.4. Rețelele Sociale

Cantitatea de informații pe care le dai despre tine pe o rețea socială nu este de neglijat. A folosi un cont pe o rețea socială pentru a accesa informații activiste, este a oferi poliției și giganților web (Google, Facebook, Twitter, Instagram, etc.) date care probabil ai dori să rămână ascunse. Rețelele sociale sunt concepute pentru a deveni rapid indispensabile și crează dependență, ceea ce este foarte periculos.

Poate părea complicat să părăsești o retea socială pe care o folosești în mod regulat ca mod de comunicare și de informare. Însă este ceea ce te sfătuim să faci. Pentru a face mai ușoară tranziția, poți să încerci să îți dai seama de ce ai impresia că ai nevoie de rețelele sociale.

Dacă folosești rețelele sociale pentru acces la informații, te sfătuim să folosești flux-urile RSS. Dacă este pentru a ține legătura cu alte colective, poți să-i întrebi dacă folosesc și alte mijloace de comunicare (mailling lists, website internet, etc.)

Dacă accepți să practici folosirea rețelelor sociale în mod curent, consolidezi puterea și priza lor asupra vieților și a organizării noastre sociale. În schimb experiențele de organizare fără ajutorul rețelelor sociale susțin ideea că dominația lor nu este inevitabilă.

Dacă folosești rețelele sociale pentru a comunica cu un numar mare de persoane într-o optică activistă, te sfătuim să publici informațiile și pe rețelele alternative pentru a nu exclude activiștii care au făcut alegerea de a nu folosi rețelele sociale uzuale.

Dacă îți place să folosești rețelele sociale pentru a rămâne în contact cu prietenii, rețeaua Mastodon este mai sigură și mai respectuoasă cu informațiile private, dar este departe de a fi perfectă (rămâne tot o rețea adictivă).

De asemenea, poți alege să-ți păstrezi totuși contul pe rețeaua de socializare, dar să nu mai publici nimic și să te conectezi doar episodic. Cu toate acestea, nu uita că rețelele de socializare sunt făcute în așa fel încât să te atragă deci această strategie poate fi complicat de pus în practică.

1.5. Metadatele de fișier

Fotografiile, fișierele PDF sau textele pot să conțină metadate care furnizează informații despre ora la care a fost făcută ultima modificare, marca aparatului de fotografiat și multe alte lucruri. Te sfătuim să ștergi de fiecare data când share-uiești un fișier. Sistemul de operare Tails conține programul Mat2 pentru ștergerea metadatelor. Acest program poate fi descărcat și pentru Linux dar poate fi folosit și direct pe web pe niște siteuri care oferă ștergerea metadatelor prin Mat2.

2. Atacuri specifice telefoanelor mobile

Vom încerca să parcurgem măsuri de protecție împotriva următoarelor atacuri :

- accesarea datelor pe care le stochează furnizorii de servicii internet,
- accesarea datelor pe care le stocheaza aplicațiile (de exemplu în cazul perchiziții telefonului confiscat de poliție),
- accesarea datelor de pe telefon de la distanță (din cauza unor erori de aplicații).

Toate aceste date pot fi recuperate în mod legal sau ilegal de poliție. Datele recuperate ilegal nu pot fi folosite ca dovezi într-un proces dar pot fi folosite pentru a te șantaja și a te constrânge la mărturii. Deci, este foarte important să nu mărturisești nimic, orice ți s-ar spune, atâta timp cât nu știi ce informații au obținut de manieră legală. Este mai bine să aștepți să vorbești cu un/o avocat/ă sau cu prietenx înainte de a determina o strategie de apărare.

2.1. Datele accessible prin operatorii de telefoane : geolocalizarea și metadatele

Tot ce spunem în acest paragraf se referă la toate telefonele mobile, smartphone sau cele mai vechi.

La fiecare 5 minute, telefonul tău trimite un semnal la antenele cele mai aproapiate (care pot să determine poziția ta prin triangularea a 3 antene) cu numărul cartelei SIM din telefon și cu numărul IMEI. Numărul IMEI este un număr de serie care identifică în mod unic telefonul.

De fiecare dată când efectuezi un apel sau trimiți un mesaj, operatorii de telefoane stochează metadatele apelului sau a mesajului timp de 2 ani. Metadatele constau în : geolocalizarea aproximativă a celor doi corespondenți, data și ora comunicării și durata apelului.

Atac posibil : recuperarea metadatelor și geolocalizarea printr-o simplă cerere.

Poliția poate cere operatorilor următoarele informații, în mod automat și rapid :
- identitatea unei persoane datorită numărului de telefon,
- factura detaliată a telefonului,
- ascultarea unui număr de telefon,
- lista numerelor de telefon care utilizează un anumit terminal de comunicații,
- privind cartelele SIM prepaid, poliția poate să afle unde a fost vânduta cartela,
- adresele IP la care un telefon se conectează.

Cum funcționează supravegherea de masă a activiștilor ?

Factura detaliată a unui număr de telefon conține o mulțime de informații care pot fi analizate cu ușurință de computer. Este un mijloc de investigație folosit des. Un exemplu de utilizare a acestor date : Fiecare persoană obține un scor de "pericol" pe baza deplasărilor sale în locuri de activiști și comunicarea cu altx activistx. În acest fel se pot detecta automat noile locuri de întalnire a activiștilor observând numărul oamenilor cu un scor mare de "pericol" care se strâng într-un loc. În mod similar, se pot detecta activistx noi prin comunicarea lor cu activistx vechi și frecventarea anumitor locuri sau localuri. Exemplu ăsta este deosebit de important pentru a înțelege că supravegherea de masă este o problemă colectivă, nu individuală.

Împotriva geolocalizării : folosește cartelele SIM cu plată în avans și nu lua întotdeauna telefonul cu tine.

Cartelele SIM pre paid au avantajul de a nu trebui să dai adevărata ta identitate. Cu toate acestea vei fi în continuare geolocalizat la fiecare 5 minute. În plus, autoritățile pot la un moment dat să asocieze identitatea falsă a cartelei SIM cu adevărata ta identitate civilă. Apeluri telefonice, schimburi de SMS și datele conecțiunilor Internet sunt printe multe alte surse de informare.

Atenție, dacă folosiți o cartelă SIM cu plată în avans cu o identitate falsă într-un telefon pe care l-ați folosit înainte, numărul IMEI rămâne același, iar in felul asta se poate face legătură între cele două identități. Dacă cumperi un telefon nou cu un mijloc de plată nominativ, numarul IMEI al telefonului va fi astfel legat de idenitatea ta. Pentru a complica munca de spionare a autorităților folosește un telefon cumpărat cash unde nu ai mai pus o cartelă cu identitatea ta adevarată.

Acest gen de soluție parțială cu cartela SIM pre paid cu nume fals poate complica semnificativ activitatea justiției. Chiar dacă serviciile de informații reușesc să facă legatura între identitatea falsă si cea adevarată, vor trebui încă să dovedească aceasta in fața judecătorilor.

Că să nu fi geolocalizatx te sfătuim să nu iei peste tot telefonul cu tine si să îl consulți mereu în într-un singur loc, ca pe un telefon fix. Atenție însa, o schimbare bruscă a obiceiurilor (de exemplu dacă îți închizi telefonul fix înaintea unui protest) sunt ușor de reperat cu o analiză automată. Mai bine lasă-l deschis la tine acasă, ca si cum ai fi rămas acasă.

A scoate cartela SIM din telefon sau a-l închide în mod regulat este un obicei destul de util.

Pentru a lăsa cât mai puține metadate, folosește aplicațiile de comunicare prin internet.

Pentru a ne proteja datele de atacurile poliției, putem să comunicăm cu telefonul, dar numai prin aplicații ca Signal, Conversation sau Element. Chiar dacă îi cere factura detaliată furnizorului tău de

servicii internet, poliția va avea acces la mai puține metadate. Furnizorul de servicii internet poate știi doar că ai cerut să comunici cu serverul Signal la un moment dat dar nu poate să știe cu cine comunici.

Împotriva ascultării telefonice, alegeți bine subiectele de discuție.

Nu ezita să întrerupi interlocutorx dacă el/ea vorbește despre un subiect delicat la telefon. Acesta nu este un mijloc deloc adecvat de comunicare pentru astfel de discuții pentru că SMS și apelurile nu sunt criptate deci vizibile de către operator și de poliție în cazul în care ești ascultatx.

Este important de știut că toate ascultările sunt salvate, stocate și pot fi folosite ani mai târziu pentru o ancheta.

2.2. Datele accessible prin aplicațiile mobile

De fiecare dată când instalezi o aplicație, acesta din urmă stochează datele despre tine pe telefonul tău precum și pe servere la distanță (pe «cloud»). Poliția poate recupera datele acestea în timpul unei percheziții sau cerând proprietarilor/dezvoltatorilor de aplicații datele pe care le au despre tine.

Aceste date ar putea fi următoarele :

- pentru aplicațiile de mesaje: toate meajele tale, eventual chiar și cele șterse,
- pentru aplicațiile GPS: toate adresele pe care le-ai introdus in GPS-ul tău precum și istoricul călătoriilor tale,
- pentru aplicațiile de cumpărături: istoricul achizițiilor, cardurile de credit înregistrate, căutările făcute,
- pentru browserele web: istoricul de navigare (chiar dacă este șters din telefonul tău dacă serverele aplicației îl stochează),
- fotografiile, videoclipurile, etc...
- contactele tale.

Măsuri de protecție : cripteaza-ți telefonul și limiteaza datele aplicațiilor.

Nu poți fi sigurx că autoritățile nu vor avea acces la datele pe care aplicațiile de pe telefonul tău le stochează. În cazul unei percheziții de telefon, ia în considerare faptul că toate datele din telefon sunt accesibile autorităților dacă doresc. Poţi încerca să limitezi accesul la informații cât mai mult posibil, alegând să criptezi telefonul cu o parolă de deblocare lungă. Această opțiune este disponibilă pe multe sisteme de operare. Însă criptarea datelor va fi utilă numai dacă telefonul este închis atunci cand poliția pune mâna pe el. Nu cunoaștem exact mijloacele de descifrare a smartphone-urilor pe care le au la dispoziție polițiștii și depinde de mărcile de telefoane.

Prin urmare, principala strategie de protecție este pur și simplu limitarea datelor stocate de aplicațiile telefonului. În toate aplicațiile, poți modifica setările de confidențialitate. Alege întodeauna protecția maximă.

Te sfătuim să te desparți imediat de orice telefon care a petrecut un moment în mâinile poliției departe de supravegherea ta, deoarece este posibil să fi instalat sisteme de urmărire.

Măsuri de protecție: nu vă bazați pe aplicațiile care se finanțeaza prin vânzarea datelelor userilor.

Ori de câte ori este posibil, dezactiveaza stocarea datelor în cloud. Multe telefoane și aplicații le descarcă automat. Datele ar trebui să fie stocate doar local pe telefon și nu pe servere la distanță. Poate fi mai complicat de facut cu anumite aplicații, cum ar fi cele oferite de GAFAM.

Nu poți avea niciodată încredere că aplicațiile care se finanțează prin vânzarea datelor tale că nu vor păstra istoricul datelor. Alegerea software-ului liber înseamnă să optezi pentru aplicațiile făcute de oameni care luptă pentru confidențialitate și împotriva supravegherii în masă.

Deci, pentru a instala aplicații pe Android, îți recomandăm să folosești F-Droid și nu Google Magazin Play. În mod similar, OpenStreetMap este preferat ca o aplicație GPS. Firefox sau Tor Browser ca browser web și NewPipe în loc de YouTube pentru a viziona videoclipuri.

În general, încercați să vă limitați dependența de GAFAM cât mai mult posibil. Recomandăm să limitezi pe cât posibil prezența pe rețelele sociale (Twitter, Facebook, Instagram etc.) și să nu folosești Chrome sau Gmail etc.

Există sisteme de operare libere care înlocuiesc Androidul pentru telefoane, dar pot fi mai complicat de instalat.

2.3. Controlul de la distanță al unui telefon

Părăsim domeniul supravegherii în masă pentru supravegherea individuală. Aceasta diferență este crucială, deoarece marea majoritate a monitorizării este automatizată. În comparație, supravegherea individuală care necesită mai multe resurse umane este mult mai costisitoare de configurat și, prin urmare, mai rară.

Serviciile de informații au avut mijloacele necesare pentru a prelua pe deplin controlul telefoanelor de la distanță și probabil le mai au și astăzi. Nu se știe exact dacă acest lucru este ușor sau nu, dacă este frecvent sau nu și depinde de mărcile telefoanelor, dar este posibil.

Acest atac permite, printre altele:
- accesul la tot ce scrii în telefon (parole etc.),
- activarea microfonului la distanță,
- activarea camerei la distanță.

În fața acestui atac, nu sunt multe de făcut. Putem încerca să-l prevenim prin instalarea a cât mai puținor aplicații posibil și prin dezactivarea Bluetooth-ului. Acest atac are loc din cauza defectelor în securitatea Bluetooth sau a unei aplicații pe care atacatorul o sparge în telefon. Atacatorii îți pot sparge telefonul și trimițându-ți un SMS cu un link ca pentru software-ul Pegasus[4].

De asemenea, poți ascunde camerele telefoanelor cu un autocolant pentru a evita, în cazul in care cineva ți-a hackuit telefonul, să facă fotografii sau videoclipuri fără să știi.

A nu folosi telefonul sau a nu-l avea cu tine sau chiar a-l folosi cât mai puțin posibil sunt cele mai bune metode de protecție împotriva acestui atac.

[4] Pegasus este un software făcut de o firma izraeleană și folosit în toata lumea pentru a spiona personalități și diverși dirigenți. https://ro.wikipedia.org/wiki/Pegasus_(spyware)

2.4. Concluzie: telefonul, un obiect care cu greu poate fi protejat

După cum am văzut, telefoanele nu vor fi niciodată ”sigure”. Orice ai face, o cartelă SIM activă este geolocată la fiecare 5 minute, ceea ce este suficient pentru a avea acces la o cantitate impresionantă de informații, chiar dacă această cartelă SIM nu este legată de identitatea ta reală (cu toate acestea, poate să fie mai târziu dacă poliția reușește într-o zi să îți verifice diferitele identități digitale și civile).

Este mai bine să eviți să citești mailurile pe telefon dacă ai un computer accesibil pentru a face acest lucru, mai ales dacă folosești sistemul de operare Tails (vedeți mai târziu).

Aplicații precum Signal ajută la evitarea supravegherii în masă prin facturi de telefon detaliate, dar nu garantează comunicații private cu alte persoane în cazul în care un telefon dintre cele cu care comunici a fost hackuit.

Cel mai bine este să eviți utilizarea telefoanelor și să ai nevoie de ele cât mai rar pentru organizarea unor activități delicate. Un sfat de bază este să nu îți iei telefonul la proteste sau alte acțiuni. Pe de o parte pentru a evita urmarirea prin geolocalizare si pe de altă parte telefonul poate fi folosit împotriva ta dacă ai fost reținutx în arest.

Biblioteca Anarhistă

Anonim
Ghid de supraviețuire digitală
2021

broșura "Guide de survie en protection numérique à l'usage des militant·es", infokiosques.net

ro.theanarchistlibrary.org