

L'ARMATURA DIGITALE

Manuale di sopravvivenza e autodifesa
per giornalisti e attivisti.



IL SENSO DELLA SICUREZZA

La sicurezza non è un prodotto software, è una pratica culturale.
Si regge su tre pilastri:



Consapevolezza
e abitudini
(La prima linea)

Strumenti e
difese invisibili
(Cifratura, 2FA)

Regole e protocolli
condivisi nel
collettivo

PEBKAC

(Problem Exists Between
Keyboard And Chair).
Gli attacchi moderni
colpiscono la mente
prima della macchina.

CONOSCI TE STESSO (THREAT MODELING)

1. GLI ASSET (Cosa proteggero?)

Identità delle fonti, documenti inediti, la mia rete di contatti.



2. GLI AVVERSARI (Chi lo vuole?)

Attori statali, cybercriminali, troll organizzati, corporazioni.



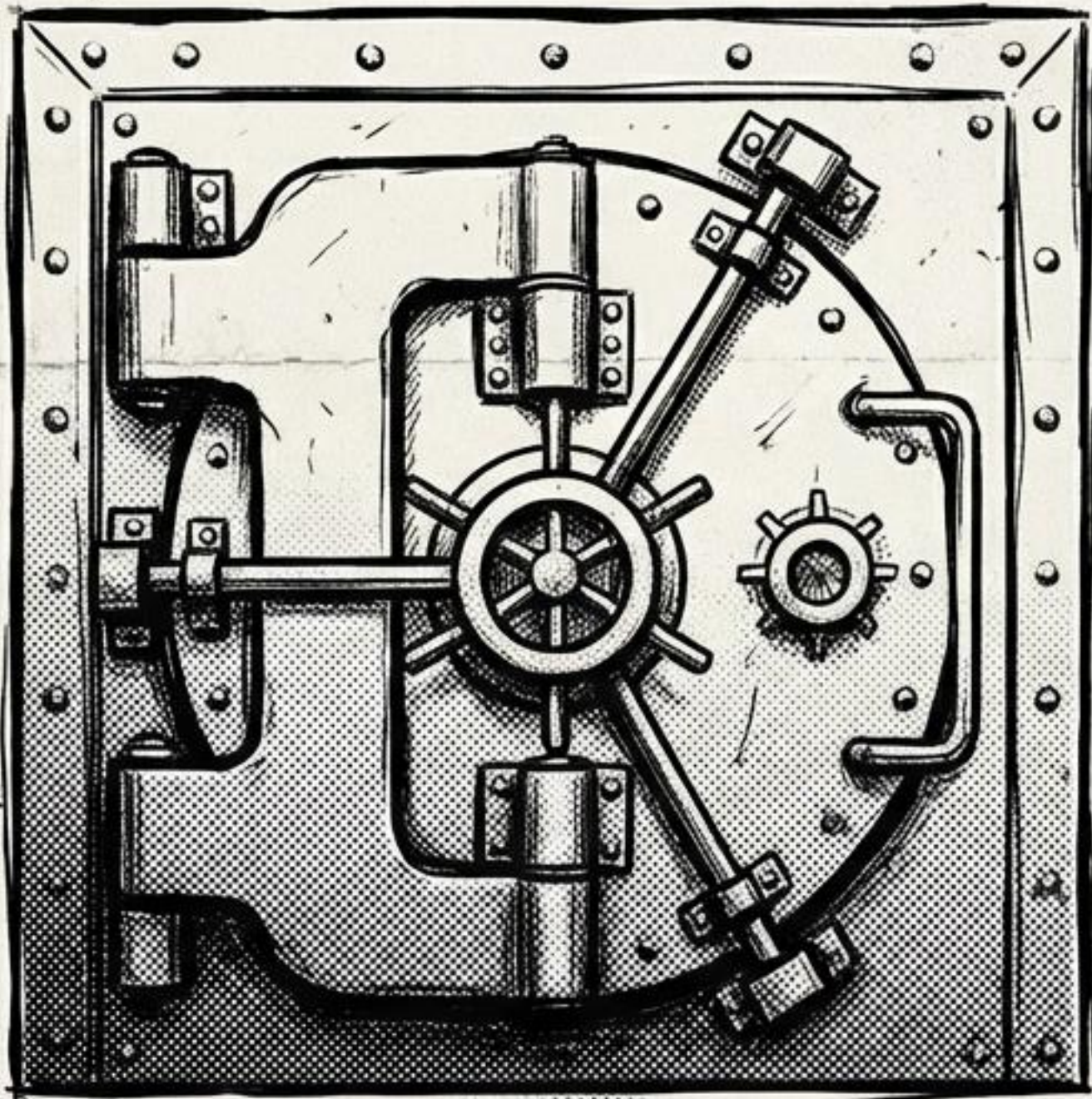
3. LA SUPERFICIE D'ATTACCO (Come ci arrivano?)

Dispositivi confiscati alla frontiera, phishing, intercettazioni di rete.

NOTA: La sicurezza non è assoluta, è proporzionata alla tua minaccia reale.

LA PRIMA LINEA: L'EMAIL

L'email è l'hub centrale. Se cade, l'attaccante può resettare le password di tutti i tuoi account.



PASSPHRASE > PASSWORD

Usa frasi lunghe (es. IlGattoVerdeVola\$I9999) invece di parole complesse ma brevi.

AUTENTICAZIONE A DUE FATTORI (2FA) MANDATORY

OTTIMO: Chiavi Hardware
(resistenti al phishing).

BUONO: App di Autenticazione
(es. Google Authenticator).

~~**PERICOLOSO:** SMS.~~
(I messaggi di testo sono
"cartoline" intercettabili).

INGEGNERIA SOCIALE & ILLUSIONI SOCIAL

I criminali non forzano i sistemi, ingannano te.

URGENZA

(Agisci ora
o perdi tutto!)



AUTORITÀ

(Finto capo
o polizia)

(Finti interessi
in comune)

SIMPATIA

REGOLA D'ORO: L'amico del tuo amico sui social NON è tuo amico. Valuta criticamente ogni richiesta e separa i profili lavorativi (pubblici) da quelli personali (blindati).

IL PROBLEMA DEL PRIMO CONTATTO

Il momento più pericoloso per una fonte è il primo “ciao”.
Una volta stabilito il canale, è facile proteggersi.
Ma il primo approccio lascia una traccia indelebile.



LA FONTE



IL GIORNALISTA

AZIONE: Pubblicizza canali multipli e sicuri (Signal, ProtonMail, SecureDrop).
Fai scegliere alla fonte lo strumento più adatto alle sue competenze.

NON TUTTE LE CIFRATURE SONO UGUALI

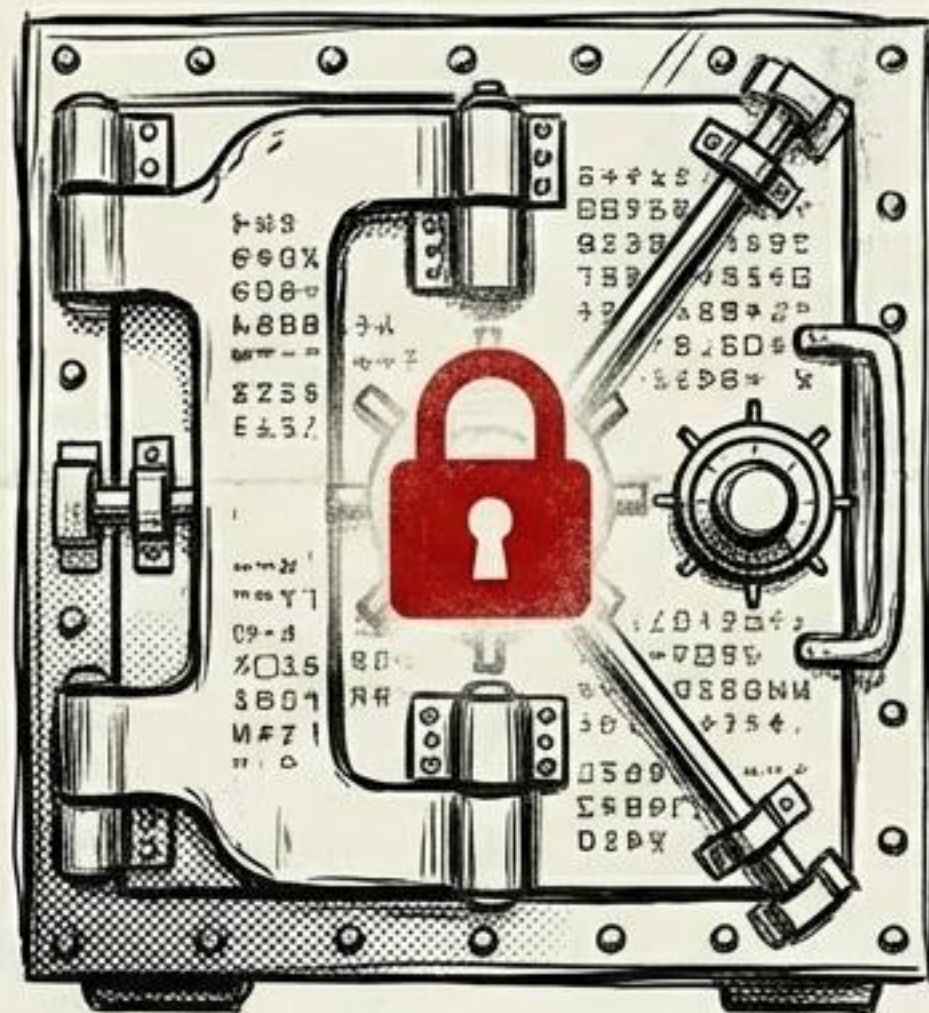
APP	E2E DEFAULT	OPEN SOURCE	METADATI
SIGNAL	✓	✓	Minima ← Il Gold Standard.
WHATSAPP	✓	✗	Alta (sanno con chi parli) ← Ecosistema chiuso e commerciale.
TELEGRAM	(Solo chat segrete) ✗	(Server proprietario) ✗	Alti ← Falso senso di sicurezza.
THREEMA / WIRE	✓	✓	Minima ← Alternative anonime (nessun numero richiesto).

LA REGOLA AUREA: CIFRARE IL DISCO

Se ti rubano il dispositivo,
non devono rubare la tua vita.

NON CIFRATO

(Basta una
spallata)



FULL-DISK ENCRYPTION

(I dati diventano
illeggibili)

- Attiva BitLocker (Win), FileVault (Mac) o LUKS (Linux).
- Usa un codice alfanumerico lungo (>12 caratteri), non un semplice PIN.

PERICOLO AFU (After First Unlock):
Anche se cifrato, dopo il primo
sblocco il telefono mantiene
le chiavi in memoria.
Alla frontiera: SPEGNI IL TELEFONO.



LA REGOLA DEL TRE (BACKUPS)

I dati non esistono se non esistono in almeno tre posti diversi.



Device



I TUOI DATI



Copia remota
Cloud



Hard Disk
esterno
cifrato

AVVERTENZA CLOUD:

Google Drive cifra solo in transito.
Usa strumenti come CryptoMator per cifrare i file prima di caricarli.

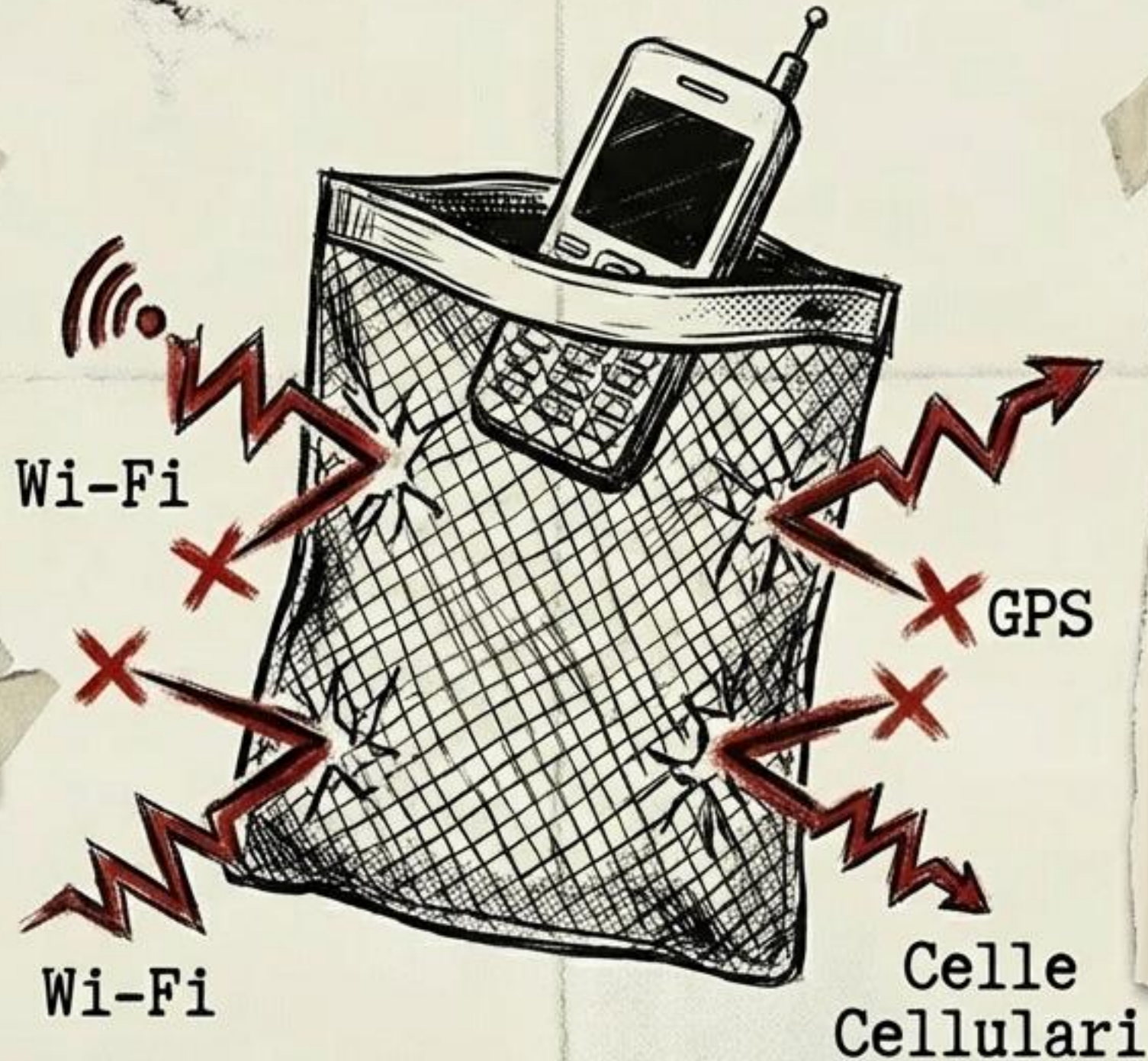
- 3 Copie totali dei dati.
- 2 Supporti fisici diversi.
- 1 Copia remota offsite.

COMPARTIMENTAZIONE E VIAGGI

Minimizzare i dati equivale a minimizzare il danno.

DISPOSITIVI BURNER

Usa telefoni
usa-e-getta o
“puliti” per
manifestazioni e
viaggi internazionali
ad alto rischio.



LA BORSA FARADAY

Riponi i
dispositivi
in una Faraday Bag
quando ti sposti.

Blocca le emissioni,
impedendo il
tracciamento GPS
e la connessione
a torri malevole.

IL NEMICO INVISIBILE: SPYWARE

Armi digitali mercenarie (come Pegasus) usate contro giornalisti e attivisti.

Si installano sfruttando vulnerabilità invisibili, spesso senza che l'utente debba cliccare su nulla (es. ricevendo un PDF su WhatsApp o un iMessage).

L'IMPATTO: Controllo totale e silenzioso. Leggono chat cifrate, accendono il microfono, tracciano la posizione e scaricano i file.



**LA MINACCIA
ZERO-CLICK**

RIDURRE IL BERSAGLIO

Contro gli attacchi Zero-Click, devi ridurre le “porte” d’ingresso.



GRANDE BERSAGLIO



BERSAGLIO RIDOTTO



BERSAGLIO MINIMO - PROTEZIONE MASSIMA

Rimuovi app inutilizzate e riduci drasticamente i permessi (fotocamera, microfono, posizione).

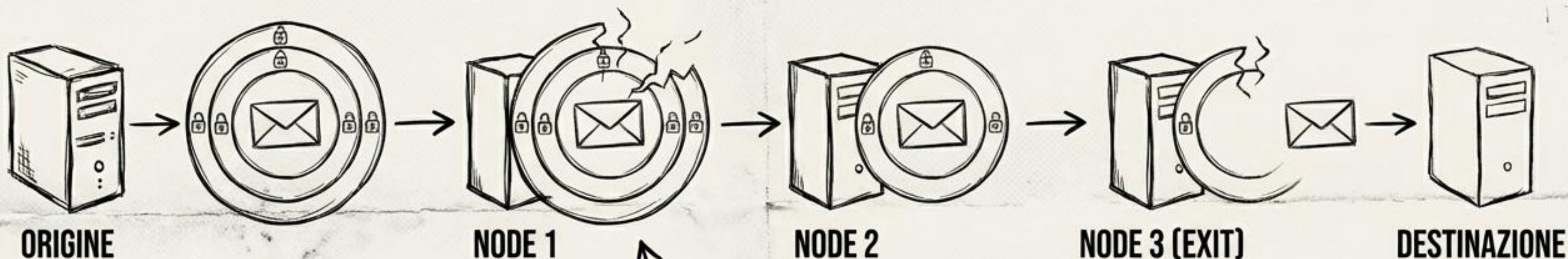
ROMPERE IN CASO DI EMERGENZA

MODALITÀ ISOLAMENTO (Apple) / PROTEZIONE AVANZATA (Android)

Limita severamente le funzionalità del telefono, bloccando allegati, anteprime web e connessioni in background. È il compromesso necessario per chi è ad alto rischio.

L'ANONIMATO (TOR & GLOBALEAKS)

La **privacy** nasconde **COSA** fai. L'**anonimato** nasconde **CHI** sei.



WHISTLEBLOWING: GlobaLeaks e SecureDrop usano Tor per ricevere documenti garantendo l'anonimato totale della fonte.

AVVERTENZA: Richiede disciplina. Non installare plugin o aprire file scaricati mentre sei su Tor.

PROTOCOLLO DI EMERGENZA

(“Mi hanno hackerato!”)



NON SPEGNERE!

Spegnere
cancella le prove
in RAM e allerta
l'attaccante.

1. ISOLA

Togli la SIM,
disattiva
Wi-Fi e
Bluetooth.
Ferma
l'emorragia
senza
spegnere.

2. ABBANDONA

Il dispositivo
è una scena
del crimine.

Passa a un
device sicuro.

3. PROTEGGI

Dal device
sicuro,
cambia password
e forza il
logout
globale.

4. AVVISA

Informa
immediatamente
le fonti a
rischio.

5. CHIAMA I RINFORZI

Contatta
esperti
forensi.

LA SICUREZZA È LIBERTÀ D'AZIONE

La sicurezza digitale non è paranoia. È lo scudo che ti permette di fare inchieste, organizzare il dissenso e proteggere la verità senza paura.



RISORSE SOS (Salva questi contatti):

- Access Now (Helpline h24)
- Citizen Lab (Supporto contro spyware)
- Electronic Frontier Foundation (EFF)
- Osservatorio Nessuno (Supporto in Italia)