Sicurezza digitale per azioni con rischio di arresto

ACTIVIST CHECKLIST

Ultimo aggiornamento: **30 ottobre 2026** Tempo stimato: circa **20 minuti**

Tradotto automaticamente: Questa pagina è stata tradotta automaticamente. Finora solo il 0% della pagina è stato revisionato da una persona. Il resto del testo potrebbe contenere errori. Aiutaci a revisionare questa traduzione.

Questa guida parla di sicurezza digitale nel caso in cui tu debba portare il telefono a un'azione nonviolenta di disobbedienza civile (detta anche azione diretta) in cui alcune persone hanno deciso di rischiare l'arresto. È solo una parte di ciò che serve per proteggere il tuo gruppo. La vostra azione dovrebbe anche prevedere un piano per la sicurezza fisica, avere un team di sicurezza e assicurarsi che tuttə conoscano i propri diritti. La nostra checklist di sicurezza per chi organizza azioni può aiutarti con tutto questo.

Valuta il tuo livello di rischio: questa guida è per azioni in cui corri un rischio legale relativamente basso (per esempio: un sit-in o incatenarti a una porta). Se stai pianificando qualcosa in cui punti all'anonimato o in cui le conseguenze legali sono molto più pesanti, dovresti prendere molte più precauzioni di quelle indicate in questa guida.

Questa guida è pensata per questa situazione:

- È un'azione organizzata in modo abbastanza centralizzato da poter stabilire accordi sulla sicurezza digitale che tuttə rispetteranno.
- Hai incoraggiato la maggior parte delle persone che partecipano all'azione a **non portare il telefono**
- Alcune persone hanno comunque bisogno del telefono per coordinare l'azione (ad es.: referente tattico, medici di piazza, squadra di de-escalation, ecc.)
- Il rischio di arresto è alto, oppure avete deciso di rischiare l'arresto.
- Pensi che gli sbirri potrebbero usare strumenti per forzare i telefoni per accedere ai dati sui telefoni che sequestrano.
- Non ti preoccupa la sorveglianza durante il tragitto verso l'azione e al ritorno.

Se qualcuno di questi punti non vale per la tua azione, potresti dover prendere più precauzioni. Dai un'occhiata alla sezione sulla sicurezza avanzata del telefono per le proteste oppure valuta di portare un telefono secondario (a volte chiamato " burner phone" o telefono usa e getta).

Consiglio per chi organizza: nei giorni che precedono l'azione, valuta di organizzare un security party così il tuo gruppo affronta questi passaggi insieme prima del giorno stesso.

Perché è importante?

Sappiamo che da decenni i movimenti sociali vengono sorvegliati, infiltrati, screditati e ostacolati da agenti governativi (sbirri locali, FBI, CIA, NSA, ecc.). Con la diffusione della tecnologia, siamo tuttə tracciatə e profilatə (anche se non sei mai statə arrestatə).

Anche quando esercitiamo i nostri diritti legali alla libertà di parola e di riunione, ci sono tante forze governative che vogliono schiacciare il dissenso e criminalizzare chi fa attivismo. (Vedi il caso Minnesota 15)

Ma ci sono cose che possiamo fare per proteggere i nostri movimenti! Questa guida propone alcune semplici azioni che tuttə possiamo fare prima e durante una protesta/azione per tenere più al sicuro noi stessə e le persone più a rischio nei nostri movimenti. Prendere queste precauzioni aiuta a proteggere tutte le persone con cui ti organizzi (non solo te e i tuoi dati). Non è un segno né un'ammissione di aver fatto qualcosa di sbagliato.

Minacce da considerare

- **Sequestro e perquisizione del telefono** - Se vieni arrestatə, gli sbirri possono provare a forzare il tuo telefono per accedere a messaggi, foto e altre informazioni private da usare come prove
- **Sorveglianza delle comunicazioni** - Gli sbirri possono intercettare normali SMS e chiamate per raccogliere informazioni sui piani della protesta e su chi partecipa
- **Richiesta giudiziaria dei dati del tuo account o del tuo operatore telefonico** - Gli sbirri possono ottenere un ordine del tribunale per accedere ai tuoi account online (come Google o Apple) o ai dati sulle tue comunicazioni e sulla tua posizione dal tuo operatore telefonico.
- **Infiltrati e agenti sotto copertura** - Alcune persone presenti alle tue riunioni o nelle tue chat di gruppo potrebbero riferire agli sbirri quello che vedono e leggono
- **Mappatura delle reti attiviste** - Ottenendo i dati dal telefono di una sola persona, gli sbirri possono identificare intere comunità di attivistə e organizzatorə collegatə a lei

Per chiunque partecipi all'azione

Importante Mettetevi d'accordo come gruppo: chi rischia l'arresto consegna il telefono a una persona di supporto (o lo lascia a casa)

Telefoni spenti e meno a rischio di sequestro aiutano a tenere tutte le persone più al sicuro.

Per le azioni con un rischio di arresto più basso, la cosa migliore è che tutte le persone A) lascino il telefono a casa oppure B) **spengano il telefono** e lo affidino a una persona di supporto. Spesso è una persona che si occupa del supporto a chi viene arrestato. Questa persona non dovrebbe partecipare all'azione, oppure dovrebbe stare in una posizione a rischio molto basso, ai margini dell'azione.

COME STABILIRE UN ACCORDO SUI TELEFONI PER LA VOSTRA AZIONE

1. **Decidete quali ruoli hanno davvero bisogno di un telefono.** Di solito sono poche persone, come chi coordina la tattica, chi fa da tramite con gli sbirri o chi fa primo soccorso. Tutte le altre persone lasciano il telefono alla persona di supporto. Chi ha un ruolo ad alto rischio di arresto non dovrebbe portare il telefono. (Oppure dovrebbe consegnarlo subito dopo l'entrata in azione.)
2. **Prima di entrare in azione, la persona di supporto raccoglie la maggior parte dei telefoni.**
3. **Fate un piano per restituire i telefoni alle persone dopo il rilascio**. Di solito significa che chi fa jail support porta i telefoni alle persone quando vengono rilasciate.
4. **Condividete l'accordo in anticipo e ripetetelo** durante i training e il briefing dell'azione.

Consiglio: se ci sono tanti telefoni e devi verificare che ogni persona sia davvero proprietaria del telefono che indica nel mucchio, puoi chiederle di sbloccarlo davanti a te.

Usa Signal per comunicare (messaggi/chiamate) durante proteste e azioni

I messaggi con crittografia end-to-end proteggono la tua privacy dalla sorveglianza, mentre i normali SMS possono essere intercettati e letti.

DO: Installa e usa Signal (gratis) per il tuo attivismo e il tuo lavoro politico

DO NOT: Usare WhatsApp, Telegram, iMessage o i normali SMS (per il tuo attivismo)

COME INSTALLARE E USARE SIGNAL

1. Installa Signal sul tuo telefono
2. Scrivi o chiama i tuoi contatti usando il loro numero di telefono, oppure chiedi a qualcuno il suo nome utente Signal. Anche l'altra persona deve avere Signal installato.

Dai un'occhiata alla nostra Checklist per Signal per istruzioni dettagliate su come configurare Signal nel modo più sicuro possibile.

- [ ] Importante **Cambia le impostazioni predefinite così che tutte le nuove chat di Signal abbiano i messaggi effimeri attivati**

  Così tuttə sono più al sicuro se il telefono di qualcunə viene sequestrato o violato.

Il miglior passo avanti che tuttə possiamo fare nell'uso di Signal è assicurarci che i messaggi effimeri siano attivati ***di default***. La maggior parte dellə attivistə con cui parliamo non li ha attivati di default. (E quasi tuttə si dimenticano di attivarli a mano per ogni nuova chat.)

Così proteggi te stessə e anche lə altrə. Non sappiamo di chi sarà il telefono che gli sbirri sequestreranno. Anche se pensiamo di parlare di cose perfettamente legali, il governo può trovare il modo di distorcere le nostre parole per cercare di montare un caso contro di noi per il nostro dissenso

Ci sono due cose da tenere d'occhio riguardo ai messaggi effimeri:

1. **Primo, cambia l'impostazione predefinita** così che ogni chat che crei abbia questa funzione attivata.
2. **Secondo, assicurati che siano attivati nelle chat avviate da altrə:** se qualcun altrə avvia la chat, potrebbe non avere i messaggi effimeri attivati. Potresti doverli attivare tu.

COME ATTIVARE I MESSAGGI EFFIMERI

1. **Per cambiare l'impostazione predefinita:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Privacy** → **Messaggi a scomparsa** → imposta il tempo che preferisci (più lungo o più corto a seconda del rischio che sei disposta/o a correre).
2. **(Solo Android) Cambia il limite di conservazione dei messaggi:** così verranno eliminati i messaggi anche nelle chat che non hanno i messaggi effimeri attivati. (Verranno eliminati solo sul tuo dispositivo.) Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Dati e archiviazione** → **Gestisci archiviazione** → **Conserva messaggi** → imposta il periodo massimo che preferisci. Torna indietro di una schermata e attiva **Applica limiti ai dispositivi collegati**.
3. **Per cambiare le chat esistenti:** Signal → Apri la chat che vuoi modificare → Clicca sul nome della persona (o del gruppo) in cima allo schermo → **Messaggi a scomparsa** → imposta il tempo che preferisci.
4. **Elimina i vecchi messaggi/chat:** i messaggi effimeri NON si applicano retroattivamente. Quindi potresti voler eliminare le vecchie chat dal tuo telefono. Purtroppo, questo non le elimina dai telefoni dellə altrə. Quindi, se si tratta di roba molto delicata, potresti dover chiedere anche a loro di eliminare la chat a mano. (E già che ci sei, incoraggiali ad attivare i messaggi effimeri di default!)

Scegliere la durata dei messaggi effimeri: quanto tempo impostare dipende da quanto sono delicati i tuoi messaggi. Una domanda che potresti farti è: "se il dispositivo di qualcunə venisse sequestrato o hackerato, quanto è importante che questi messaggi non siano accessibili?"

- Per chiacchierare di cose a basso rischio con amicə, potresti scegliere 4 settimane.
- Per il normale lavoro di organizzazione politica, potresti scegliere 1 settimana.
- Per le azioni più a rischio, potresti impostarlo su 1 giorno, 1 ora o 5 minuti, così i messaggi spariscono prima che l'azione inizi.

Nota: i messaggi scompaiono solo dopo essere stati letti. Quindi, se chi lo riceve non lo legge per 2 settimane e hai impostato i messaggi a scomparsa su 4 settimane, il messaggio sparirà in realtà 6 settimane dopo che l'hai inviato.

Usa Proton Docs per collaborare (invece di Google Docs)

Proteggi i dati del tuo gruppo da Google che traccia ogni documento che apri

DO: Usa Proton Docs (o Cryptpad) per organizzarti

DO NOT: Usare Google Docs per organizzarti

Google traccia tutta l'attività degli utenti, compresi i documenti che apri, condividi e a cui accedi. Gli sbirri possono ottenere questi dati con mandati o citazioni, ed è già successo che li condividessero anche senza le autorizzazioni necessarie. Organizzarci fuori da Google Docs ci aiuta a proteggerci a vicenda.

Proton Docs è un'ottima alternativa a Google Docs. I tuoi documenti sono protetti con crittografia end-to-end: anche se le autorità accedessero ai server di Proton, non potrebbero vedere cosa c'è scritto nei tuoi documenti.

Proton Docs non ti rende anonimo di default! Se ti organizzi in contesti più a rischio, assicurati di conoscere i limiti di Proton e come usarlo in sicurezza.

COME USARE PROTON DOCS

1. Crea un account Proton se non ne hai già uno: scegli il piano gratuito
2. Vai su Proton Drive → Clicca sul pulsante **Nuovo** → Seleziona **Nuovo documento**
3. Quando il documento è pronto per essere condiviso, puoi cliccare sul pulsante "Condividi" e condividerlo con altri account Proton, oppure attivare "Crea link pubblico" per condividerlo con chi non ha un account Proton. Fai attenzione a dove condividi il link, perché sarà meno sicuro! Ti consigliamo di usare una password se attivi la modalità "chiunque abbia il link può visualizzare".

Incoraggia le persone con cui ti organizzi a crearsi un account Proton: così, insieme, potete diventare tutte più sicure.

Cerchi dei moduli? Proton non offre una soluzione come Google Forms. Puoi provare i moduli di Cryptpad o Jotform con l'opzione di crittografia end-to-end attivata.

Non scrivere niente che non vorresti sentirti rileggere in tribunale

Chat, documenti e appunti possono finire nelle mani degli sbirri.

DO: Parla dei dettagli delicati di persona, con i telefoni messi via

DO NOT: Scrivere nelle chat di gruppo o nei documenti condivisi chi rischia l'arresto o i dettagli del piano

Viviamo in un'epoca in cui il governo federale sorveglia e persegue chi fa attivismo con un'intensità che non si vedeva da decenni.

Quando organizziamo su larga scala, dobbiamo sempre trovare un equilibrio tra il bisogno di sicurezza e il bisogno di far crescere i nostri movimenti e costruire potere.

Un modo per ridurre i rischi inutili è fare attenzione a cosa mettiamo per iscritto. Quello che scriviamo finisce spesso per essere usato contro di noi in tribunale, anche se usiamo strumenti crittografati come Signal.

Per qualsiasi attività organizzativa che comporti il rischio di arresto (o per attività particolarmente prese di mira, come l'ICE watch o la solidarietà con la Palestina), è importante mettersi d'accordo su cosa non verrà messo per iscritto.

Come i dati finiscono in tribunale:

- **Il telefono di qualcuno viene sequestrato.** Se qualcuno in una chat viene arrestato e gli sbirri riescono ad accedere al suo telefono, possono leggere ogni messaggio e documento che contiene.
- **Un'azienda consegna il tuo account.** Servizi come Google Docs non hanno la crittografia end-to-end, quindi l'azienda può vedere i tuoi documenti e consegnarli agli sbirri se ricevono un subpoena o un warrant. Nel 2025 Google ha consegnato all'ICE i dati dell'account di uno studente di dottorato in risposta a un subpoena, senza avvisare prima

lo studente.

- **Nel gruppo c'è un informatore o uno sbirro infiltrato.** Nel processo federale del 2026 contro i Minnesota 15, agenti sotto copertura sono entrati nelle chat di gruppo Signal degli attivisti e hanno passato quello che leggevano, che l'accusa ha poi usato in tribunale.

COME TENERE I TUOI PIANI FUORI DA QUALSIASI TRACCIA SCRITTA

Evita di mettere per iscritto le cose più rischiose, che siano messaggi, documenti o anche appunti su carta.

Prima di scrivere qualcosa, chiediti: "Mi andrebbe bene sentirlo leggere ad alta voce in un processo contro di me?" Se la risposta è no, tienilo per una conversazione di persona (idealmente con tutti i telefoni e i dispositivi in un'altra stanza).

Cose che potresti voler evitare di scrivere:

- Che stai pianificando qualcosa che comporta il rischio di arresto (anche un sit-in molto tranquillo di solito viola una legge sul trespassing, cioè l'ingresso non autorizzato in una proprietà)
- Chi fa parte del gruppo o partecipa all'azione
- Chi ha un ruolo di guida
- Per le azioni: il luogo, le tattiche, le informazioni che possono identificare le persone coinvolte
- Altri gruppi coinvolti
- Battute, sfoghi o sarcasmo che potrebbero sembrare una minaccia o un'intenzione seria.

Ultimo passo: prendi l'abitudine di **cancellare o distruggere quello che hai messo per iscritto appena non ti serve più**. Questa cosa spesso viene dimenticata, quindi può essere utile prevedere dei sistemi per assicurarsi che venga fatta.

Tratta i gruppi grandi o aperti come se ci fosse dentro un informatore. Di solito non puoi sapere chi lo è. E mettersi a "cercare la spia" all'interno di un gruppo è una cattiva pratica. Più persone ci sono in un gruppo, più è difficile conoscerle tutte. Tieni le conversazioni più delicate all'interno di piccoli gruppi di persone che conosci e di cui ti fidi.

☐ Scegli un numero di telefono da chiamare se ti arrestano. Scrivilo sul corpo con un pennarello indelebile.

È il numero che chiamerai se ti arrestano, di qualcuno che può aiutarti da fuori. Vale per le situazioni a rischio più alto.

COME SCEGLIERE UN NUMERO DI TELEFONO DA CHIAMARE SE TI ARRESTANO

1. **Decidi chi chiamare se ti arrestano:**
   - Se non sai se nella tua zona c'è una linea attiva di supporto legale per chi viene arrestato, scegli una persona come contatto di emergenza e usa il suo numero. Può essere un'amica, un amico o una compagna o un compagno di fiducia che può aiutarti a trovare supporto legale. Assicurati di avere il suo consenso prima.
   - Se partecipi a un'azione a rischio più alto, chi la organizza potrebbe aver già predisposto un numero di supporto legale apposito da usare.
   - Se vivi in una grande città, potrebbe esserci una linea di supporto per chi viene arrestato gestita dalla National Lawyers Guild, con persone pronte ad aiutare chi fa attivismo. Dai un'occhiata alla lista dei numeri di supporto per chi viene arrestato della NLG qui. Ti consigliamo di usare una di queste linee solo se hai compilato prima un modulo di supporto per l'arresto, così possono chiamare i tuoi contatti al posto tuo mentre si attivano per aiutarti.
2. **Scrivi il numero di supporto legale sul corpo con un pennarello indelebile** in un punto dove non si cancella facilmente (parte alta del braccio, gamba, busto). Chiama quel numero se ti arrestano e ti concedono una telefonata.

Blindare il telefono (per chiunque porti un telefono)

Se sei tra le persone che portano un telefono e hai dati molto sensibili sul tuo telefono principale o corri un alto rischio di essere presə di mira dagli sbirri, ti consigliamo di seguire tutti i passaggi di questa guida usando un telefono secondario con meno dati.

Tieni il telefono (e il portatile) aggiornato all'ultima versione del sistema operativo

Ti protegge da hacker, spyware e dagli strumenti che gli sbirri usano per hackerare i telefoni.

DO: Installa gli aggiornamenti appena te lo chiede

DO NOT: Continuare a premere "aggiorna più tardi"

Ogni volta che esce un nuovo aggiornamento del sistema operativo, chiude delle falle di sicurezza. Ogni aggiornamento che non hai installato significa una lista più lunga di modi in cui gli sbirri possono entrare nel tuo dispositivo. Immaginalo come un grande edificio con sempre più porte lasciate aperte.

Se il tuo sistema operativo non è aggiornato, molti degli altri consigli di questa guida non proteggeranno i tuoi dati.

Inizia dal telefono. Se stai facendo qualcosa di più rischioso, assicurati di aggiornare tutti i tuoi dispositivi.

COME FARE GLI AGGIORNAMENTI

Visto che gli aggiornamenti di sicurezza sono così importanti, **abbiamo creato uno strumento che ti guida passo passo**.

Controlla gli aggiornamenti del telefono e del computer →

COME FARE GLI AGGIORNAMENTI MANUALMENTE

Se preferisci fare gli aggiornamenti a mano, ecco come fare per ogni dispositivo:

Clicca per vedere i passaggi manuali

Imposta un codice di sblocco del telefono di 8-10 cifre casuali

Agli sbirri servono anni per craccare un codice casuale di 8 cifre. Con strumenti automatici, probabilmente riescono a indovinare il tuo codice attuale in meno di 5 minuti.

DO: Usa il tuo password manager o il nostro generatore di codici integrato per creare un codice casuale da 8 a 10 cifre

DO NOT: Usare un codice che hai inventato tu (date, sequenze sulla tastiera, ecc.). Se puoi, non usare codici di sblocco a 6 cifre.

COME CAMBIARE IL CODICE DI SBLOCCO

1. **Scegli un codice casuale lungo da 8 a 10 cifre.** Il modo più sicuro per generare un codice casuale è usare la funzione di generazione di password casuali del tuo password manager (impostala su solo numeri), ma puoi anche usare il nostro generatore di codici. (Noi umani non siamo bravi a inventare codici casuali, quindi ti consigliamo di non provare a pensarne uno da te.)
2. Cambia il codice di sblocco:

   IPHONE

   Impostazioni → **Face ID e codice** → **Cambia codice** → **Opzioni codice** → **Codice numerico personalizzato**

   ANDROID

   Impostazioni → **Sicurezza** → **Blocco schermo** → Inserisci il blocco attuale → **PIN/Password** → Inserisci un codice
3. **Esercitati con il nuovo codice** almeno 10 volte di fila adesso, così sarà più facile ricordarlo. (Se disattivi lo sblocco con il volto o l'impronta digitale, dovrai inserire il codice ogni volta che apri il telefono.)
4. Scrivi il nuovo codice su un foglio e tienilo in un posto sicuro a casa finché non l'hai memorizzato. Poi distruggilo dopo 2-3 settimane. Può esserti utile impostare un promemoria sul telefono.

Per una sicurezza in più, usa un cronometro per scegliere le tue cifre casuali

Quanto ci vuole per craccare un codice?

TIPO	TEMPO NECESSARIO PER CRACCARLO (MEDIA)	ESEMPIO
Sequenza di 6 cifre *facile da indovinare*	**Meno di 24 ore** per craccarlo	*333666 (sequenza comune)* oppure *110582 (data nel formato statunitense per il 5 novembre 1982)*
Codice *casuale* di 6 cifre	**200 giorni** per craccarlo	*238253*
Codice *casuale* di 8 cifre	**Oltre 40 anni** per craccarlo	*34780026*

Nota: questi tempi valgono solo per i telefoni. I computer si possono craccare molto più in fretta e hanno bisogno di password molto più robuste.

Fonti: le stime nella tabella qui sopra si basano sul numero di tentativi al secondo effettivamente osservati con gli strumenti di hacking forense usati dagli sbirri. Se ti serve più sicurezza, usa un codice di 10 cifre: ti protegge anche negli scenari di cracking più estremi. Trovi le fonti nelle FAQ sui codici di sblocco qui.

☐ Disattiva lo sblocco con volto/impronta (biometrico)

Con un codice di sblocco hai più tutele legali rispetto allo sblocco biometrico. Gli sbirri possono provare a costringerti a sbloccare il telefono con i dati biometrici.

COME DISATTIVARE LO SBLOCCO CON VOLTO/IMPRONTA

IPHONE

Impostazioni → **Face ID e codice** → Disattiva **Usa Face ID per: Sblocco di iPhone**

(Il resto puoi lasciarlo attivo.)

ANDROID

Impostazioni → **Schermata di blocco** (o **Sicurezza**) → **Dati biometrici e sicurezza** → **Disattiva sia il Riconoscimento del viso sia lo Sblocco con impronta digitale** per sbloccare il telefono

Attenzione però: lo sblocco con volto e impronta ti permette di usare password più forti senza doverle digitare ogni volta. Se devi scegliere, è meglio avere un codice di sblocco più lungo che disattivare lo sblocco con volto/impronta. Se lasci attivi i dati biometrici, assicurati di sapere come disattivarli in fretta se stai per entrare in una situazione ad alto rischio

(vedi i consigli qui sotto).

- **Spegnere completamente il telefono è il modo migliore per disattivare temporaneamente i dati biometrici**, perché in questo modo vengono anche cifrati i tuoi dati. Al prossimo sblocco servirà il codice.

- **Consiglio per bloccare l'iPhone:** se lasci attivo lo sblocco con volto/impronta, puoi fare in modo che al prossimo sblocco serva il codice **premendo 5 volte il tasto laterale**.

- **Consiglio per la fotocamera dell'iPhone:** puoi scattare foto senza sbloccare il telefono **scorrendo verso sinistra** sulla schermata di blocco. (Nel caso ti arrestino mentre stai filmando.)

- **Consiglio per la fotocamera Android:** su molti telefoni Android puoi aprire la fotocamera senza sbloccare il telefono **premendo due volte il tasto laterale/di accensione**.

Esci dai gruppi Signal che potrebbero mettere a rischio altre persone

Così proteggi la tua rete se ti sequestrano il telefono.

Se gli sbirri ti sequestrano il telefono, uno dei rischi più grandi è esporre tutta la tua rete. Anche se le persone non usano il loro vero nome sull'account Signal, dietro ogni nome utente Signal c'è comunque un ID univoco. E gli sbirri possono usarlo per collegare l'identità di qualcuno attraverso tanti dispositivi sequestrati.

Devi sia uscire dal gruppo SIA eliminarlo:

- Se esci soltanto dal gruppo, sul tuo telefono restano i vecchi messaggi e la cronologia di chi faceva parte del gruppo.
- Se elimini soltanto il gruppo, continueranno ad arrivare nuovi messaggi e la chat ricomparirà.

COME USCIRE DA UN GRUPPO SIGNAL ED ELIMINARLO

1. **Organizzati per rientrare dopo:** quando stai per affrontare una situazione in cui potresti essere arrestatə, fai una lista su carta, a casa o in un posto sicuro, di tutti i gruppi e delle persone a cui scrivere per farti riaggiungere dopo l'azione o dopo aver passato il confine.
2. **Per uscire dal gruppo:** Signal → [Gruppo] → Tocca l'icona del gruppo in alto → **Abbandona il gruppo**
   - Se sei l'unicə admin, devi rimuovere tutti i membri oppure nominare un altrə admin.
3. **Per eliminare il gruppo dal tuo telefono:** Signal → Schermata principale → Scorri verso sinistra sulla chat → **Elimina**
   - Il gruppo non verrà eliminato per nessun altro.

Consigli di igiene digitale:

- Imposta un promemoria ricorrente per fare pulizia nelle tue chat Signal ogni 3 mesi.
- Assicurati di segnarti da quali gruppi esci e a chi puoi chiedere di riaggiungerti dopo l'azione.

Nota: se trovi questo procedimento parecchio fastidioso e macchinoso (perché lo è!), è un altro buon motivo per usare un telefono secondario durante le azioni. Quel telefono starebbe solo nell'uno o due gruppi necessari per portare a termine l'azione di quel giorno.

Durante l'azione (se hai portato un telefono)

Importante Spegni completamente il telefono se il rischio di arresto sta aumentando

I tuoi dati sono più protetti quando il telefono è spento (non solo bloccato)

Quando il telefono è completamente spento, è più protetto contro l'estrazione dei dati da parte degli sbirri. I dati restano crittografati finché non inserisci il codice di sblocco per la prima volta.

Quindi, la cosa più importante che puoi fare per proteggere i tuoi dati è spegnere il telefono appena pensi che il rischio di arresto stia aumentando.

COME SPEGNERE IL TELEFONO

1. IPHONE
   premi **5 volte** il tasto laterale di blocco schermo per far apparire subito l'opzione **Spegni**

   ANDROID
   tieni premuto il tasto di accensione finché non appare il menu di spegnimento → tocca **Spegni**
2. **Esercitati** a farlo più volte, così riuscirai a farlo in fretta.
3. Durante una situazione ad alto rischio, **ricorda alle persone vicino a te** di spegnere anche i loro telefoni.

Pro e contro: sappiamo che spegnere il telefono ha i suoi pro e contro. A volte è più importante filmare gli sbirri o coordinarsi con chi è al nostro fianco. Pensa bene a qual è la tua priorità. Se devi filmare, valuta di portare un telefono secondario, così avrai meno dati sensibili con te.

Affida il telefono a qualcunə che non rischia l'arresto

Non avere il telefono con te quando vieni fermatə è il modo migliore per proteggere i tuoi dati e il movimento. Spegnerlo del tutto è la seconda opzione migliore.

COME AFFIDARE IL TELEFONO A QUALCUNƏ CHE NON RISCHIA L'ARRESTO

- **Se metti in conto di rischiare l'arresto**: spegni il telefono e consegnalo alla persona di supporto che avete scelto prima di entrare in azione.
- **Se ti serve il telefono durante l'azione**: chi ha un ruolo di supporto (tattico, medico, de-escalation, ecc.) potrebbe aver bisogno del telefono durante l'azione. A seconda di come è organizzata l'azione e di quanto sono imprevedibili gli sbirri, queste persone potrebbero non riuscire ad andarsene quando il rischio di arresto aumenta.
  - Se l'organizzazione dell'azione lo permette e ti serve il telefono fino all'ultimo minuto, affidalo a qualcunə.
  - Se ti serve il telefono e non puoi affidarlo a nessunə, assicurati di spegnerlo del tutto prima dell'arresto.

Dopo l'azione

Dopo l'azione, elimina i documenti di pianificazione e i gruppi Signal

Le vecchie chat e i vecchi documenti si possono ancora leggere se un telefono viene sequestrato o se in seguito arriva un mandato di comparizione per un account.

Una volta finita l'azione, i documenti e le chat che avete creato non servono più. Più a lungo restano in giro, più è probabile che finiscano nelle mani degli sbirri tramite un telefono sequestrato, una subpoena o un infiltrato nel gruppo.

Prima dell'azione, mettetevi d'accordo su un piano di pulizia. Create un sistema per responsabilizzarvi a vicenda e portarlo a termine.

Se qualcuno è stato arrestato o incriminato, consultate il vostro team di supporto legale o un avvocato prima di eliminare qualsiasi cosa. Eliminare dei dati quando sapete già di un'indagine, di una subpoena – cioè un mandato di comparizione – o di accuse può essere considerato distruzione di prove, che è un reato a sé. Anche per questo conviene attivare i messaggi a scomparsa con un timer breve prima dell'azione, così la maggior parte dei messaggi sarà già sparita.

COME FARE PULIZIA DOPO UN'AZIONE

1. **Elimina i documenti.** Questo include i documenti di pianificazione, i documenti Proton/CryptPad, i fogli di calcolo, i moduli per il supporto alle persone arrestate e qualsiasi appunto scritto. Poi svuota il cestino.
2. **Chiudi i gruppi Signal**: i gruppi Signal possono essere utili per l'organizzazione continuativa, ma l'elenco dei membri è anche un rischio per tutte le persone se in futuro il telefono di qualcuno viene sequestrato. Valuta di spostare tutte le persone in un gruppo più grande solo per annunci per l'organizzazione continuativa, invece di tenere in vita quel piccolo gruppo.
   - Scrivi un messaggio per avvisare tutte le persone che il gruppo sta per chiudere e chiedi di eliminare la chat dai loro telefoni. Rimuovi tu stessə ogni membro per essere sicurə che succeda davvero.
   - Elimina la chat dal tuo telefono: Signal → Schermata principale → Scorri verso sinistra sulla chat → **Elimina**. (Questo non rimuove il gruppo dai telefoni delle altre persone, solo dal tuo. I messaggi a scomparsa, però, si cancelleranno automaticamente dai telefoni di tutte le persone.)
3. **Se non sei admin,** esci dal gruppo E eliminalo e incoraggia tutte le altre persone a fare lo stesso.
4. **Distruggi con il trituratore tutti gli appunti cartacei**, le mappe o gli elenchi.

Per saperne di più

- CLDC - Aspettati l'inaspettato: proteggi il tuo telefono in caso di sequestro o smarrimento (2021, in inglese)
- Freedom of the Press Foundation - Cosa fare se gli sbirri ti sequestrano il telefono (2016, in inglese)

Continua a imparare con queste guide correlate

Checklist di sicurezza per chi organizza azioni

Sicurezza fisica, digitale e legale per chi organizza azioni di disobbedienza civile in cui si rischia l'arresto.

Organizza un incontro sulla sicurezza

Un programma tipo per affrontare le checklist insieme al tuo gruppo.

Preparati per una manifestazione

Per chiunque partecipi a una manifestazione.