Checklist per difendersi dal doxxing

ACTIVIST CHECKLIST

Ultimo aggiornamento: **22 maggio 2026** Tempo stimato: circa **45 minuti per le protezioni di base**

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.

Il **doxxing** è quando chi ti molesta raccoglie e pubblica informazioni che ti identificano personalmente, con l'obiettivo di molestarti o intimidirti. Spesso porta a molestie online e può far perdere il lavoro, avere conseguenze legali (abbiamo visto l'ICE usare dati raccolti in questo modo per arrestare persone) e, in rari casi, causare danni di persona.

Le informazioni diffuse possono includere nome e cognome legali, indirizzo di casa, posto di lavoro, numero di telefono, email, foto, familiari e così via.

Perché è importante: chi ci si oppone usa il doxxing e le molestie online perché vuole *seminare paura* e spingerci a smettere di fare il nostro lavoro. Più ci difendiamo in anticipo, più possiamo essere forti nelle nostre azioni. Se aspetti di subire il doxxing, le informazioni saranno già in giro e fuori dal tuo controllo.

Come il doxxing si trasforma in molestie e danni

Esempi di molestie che possono derivare dal doxxing: dopo che le tue informazioni sono state diffuse, ecco il tipo di molestie che potresti subire: email/messaggi molesti, tentativi di hackerare i tuoi account online, pacchi spediti al tuo indirizzo, qualcunə che si spaccia per te online, attacchi al tuo datore di lavoro per rovinarti la reputazione o farti licenziare, tentativi di aprire carte di credito a tuo nome, le tue informazioni passate all'ICE o agli sbirri per farti arrestare, oppure uno qualsiasi di questi attacchi contro la tua famiglia o le persone che ti sono vicine.

La maggior parte dei casi di doxxing resta online. I rari casi in cui la cosa si è spostata nel mondo reale hanno incluso atti vandalici contro proprietà, aggressori che si presentano a casa tua o sul posto di lavoro per molestarti, il noleggio di un "camion del doxxing" per screditarti in pubblico, lo swatting (chiamare una squadra SWAT contro di te) e, cosa più grave di tutte, funzionari governativi che usano i dati raccolti per arrestare persone. Sono cose poco probabili, a meno che tu non sia una figura pubblica.

Strade che un aggressore potrebbe usare:

- Potrebbero cercare il tuo nome sui motori di ricerca (come Google) o sui social
- Potrebbero cercarti su LinkedIn o trovare una copia del tuo curriculum per scoprire dove lavori, dove studi e il tuo percorso professionale
- Potrebbero usare le foto che hai pubblicato online per capire dove vivi o dove passi il tuo tempo
- Potrebbero cercarti sui siti di "ricerca persone" per risalire al tuo indirizzo partendo dal tuo nome o numero di telefono
- Potrebbero cercare il tuo numero di telefono su Venmo per capire dove passi il tuo tempo in base a chi paghi e quando
- Potrebbero usare una tua foto (trovata online o scattata a una manifestazione) per fare una "ricerca inversa per immagini" e trovare i tuoi profili online.

Poi possono diffondere queste informazioni pubblicamente in vari modi: su "siti di doxxing" pubblici (ad es. Canary Mission, sui social o in canali semi-pubblici come Telegram e i forum del dark web.

Come possiamo proteggere noi stessɜ e la nostra comunità

Cosa vogliamo proteggere: il nostro obiettivo è rendere molto più difficile raccogliere le tue informazioni personali e sensibili, partendo da quelle più delicate: il tuo indirizzo di casa e il tuo posto di lavoro.

Fatelo insieme. Molti gruppi che lavorano pubblicamente affrontano questa checklist con un security party, così tuttə si mettono al sicuro nello stesso momento.

Facciamo questo lavoro perché vogliamo trasformare i sistemi e la cultura. Leggendo guide come questa è facile pensare: "Devo nascondere tutto e non uscire mai più di casa". È proprio questo tipo di paura che chi ci si oppone spera di provocare minacciandoci abbastanza. Ti invitiamo invece a usare queste misure di difesa per darti la forza di **continuare ad agire con coraggio**.

Più il tuo lavoro ha successo, più è probabile che prima o poi tu debba affrontare qualche forma di doxxing o di molestie online. Consideralo un segno che sei sulla strada giusta.

Stai subendo doxxing o molestie online in questo momento? Se sì, vai alla sezione su come rispondere al doxxing più sotto.

Protezioni di base

TUTTƏ Questa sezione fa per te se fai qualsiasi tipo di attivismo o advocacy che potrebbe attirare l'attenzione di chi ti si oppone.

Scopri quanto è facile trovare il tuo indirizzo di casa su Google usando solo il tuo nome o il tuo numero di telefono

Il modo migliore per capire quanto sia importante proteggere il tuo profilo pubblico è cercare te stessə.

Più avanti in questa guida ti faremo fare una ricerca manuale su Google più dettagliata. Per ora, però, **l'obiettivo è solo capire quali informazioni private su di te sono facili da trovare**.

COME FARE UNA PRIMA RICERCA SU GOOGLE DELLE TUE INFORMAZIONI PRIVATE: PROVA A TROVARE IL TUO

Cerca su Google quanto segue, sostituendo i valori di esempio con i tuoi dati reali:

- `"555-867-5309"` (il tuo numero di telefono)
- `"Jamie Garcia" address` (il tuo nome più la parola "address", cioè indirizzo)
- `"Jamie Garcia" phone number` (il tuo nome più le parole "phone number", cioè numero di telefono)
- `"Jamie Garcia" "Springfield High School"` (il tuo nome più la tua scuola superiore o università)
- `"Jamie Garcia" employer` (il tuo nome più la parola "employer", cioè datore di lavoro, oppure prova con il nome del tuo posto di lavoro)

Usare le virgolette aiuta, ma non è obbligatorio. Se non trovi niente, prova senza virgolette.

Il tuo compito: **quanto ci metti a trovare il tuo indirizzo di casa?**

Probabilmente non molto. Il resto di questa guida ti aiuterà a rimuovere buona parte di queste informazioni.

Importante Cancellati dai siti di "ricerca persone" con un servizio automatico (come EasyOptOuts)

Usare uno strumento che ti cancella automaticamente da tutti questi siti ti fa risparmiare un sacco di tempo.

DO: Iscriviti a EasyOptOuts (20 $/anno), oppure a Optery Ultimate (249 $/anno) per una copertura maggiore

DO NOT: Non consigliamo DeleteMe perché è meno efficace di EasyOptOuts

I **siti di "ricerca persone"** sono un tipo di "data broker". Raccolgono informazioni da registri pubblici e privati per creare un "profilo" praticamente di chiunque. Se hai mai avuto un numero di telefono, usato una carta di credito o votato, probabilmente sei su uno di questi siti.

Prova tu stessə: cerca il tuo nome o il tuo numero di telefono su questo sito (lo usiamo come esempio perché mostra subito i risultati senza obbligarti a registrarti). Quasi tutte le persone si stupiscono di quante informazioni siano facilmente accessibili. Altri siti importanti di questo tipo sono Whitepages, Spokeo, BeenVerified e un numero sempre maggiore di strumenti di ricerca basati sull'IA.

Perché pagare un servizio di rimozione automatica: puoi fare questo processo di "opt out" a mano, ma ci vuole un'infinità di tempo e devi rifarlo ogni pochi mesi, quando i siti dei data broker cambiano. È assurdo dover pagare per proteggere la nostra privacy, ma ci fa risparmiare un sacco di tempo da dedicare all'attivismo.

Quale strumento di rimozione automatica dovrei usare?

- **EasyOptOuts (consigliato)** - 20 $/anno - È tra i più efficaci e il più economico.
- **Optery Ultimate** - 250 $/anno - Un po' più efficace, se puoi permetterti la spesa in più. Possono usare una copia del tuo documento d'identità (con il numero del documento oscurato) per cancellarti dai siti che richiedono un documento.
- **E DeleteMe? -** È l'opzione più conosciuta, ma è riuscita a rimuovere solo il 27% dei profili, contro EasyOptOuts (65%) e Optery Ultimate (68%). (Fonte).

COME CANCELLARTI DAI SITI DI "RICERCA PERSONE" CON EASYOPTOUTS

Tempo necessario: 5–15 minuti

1. **Iscriviti a EasyOptOuts** (20 $/anno)
2. **Inserisci i tuoi dati personali:** segui le istruzioni. La cosa più importante è inserire i tuoi dati **attuali** (indirizzo, numero di telefono, email). Se non riesci a trovare tutti i tuoi indirizzi passati, non fa niente.

   > **Attenzione:** NON inserire **pseudonimi** o **numeri di telefono usa e getta** che usi solo per l'attivismo e che sono già completamente separati dalla tua vera identità. Non vorresti che finissero collegati tra loro dentro questo sistema.

3. Passa alla voce successiva della checklist per fare gli **opt-out manuali** dai siti che EasyOptOuts non riesce a gestire.
4. Valuta di chiedere anche a chi vive con te di iscriversi. Se qualcuno scopre che vivete insieme, potrebbe cercare quella persona con la stessa facilità e poi prendere di mira te.

Tempi: Le prime rimozioni possono richiedere qualche giorno, e per alcuni siti a volte anche un paio di mesi.

Per tua info: Non riceviamo nessuna commissione dai servizi a pagamento che linkiamo. Li consigliamo perché sono i più efficaci che abbiamo trovato.

Privacy di EasyOptOuts: Alcune persone sono preoccupate all'idea di inserire tutti i propri dati in un sito del genere. Nessun sito è immune dalle violazioni dei dati, ma di questo ci fidiamo in base alla sua storia e alla sua reputazione. E poi quei dati servono per fare le rimozioni.

Strumento alternativo: Kanary è un'app gratuita che cerca i tuoi dati personali su Google e ti guida passo passo nella rimozione manuale. Però richiede comunque moltissimo tempo ed è facile mollare prima di aver finito tutte le rimozioni.

- [ ] Importante **Fai manualmente l'opt-out dai siti di “ricerca persone” che non vengono coperti in automatico**

  Anche gli strumenti più efficaci per la rimozione dai "siti di ricerca persone" coprono solo il 70% dei siti.

Alcuni di questi siti rendono molto difficile rimuovere un profilo, quindi servizi come EasyOptOuts non possono farlo al posto tuo. Di solito ti chiedono di ricevere un'email per confermare che sei proprio tu a rimuovere il profilo.

COME RIMUOVERTI MANUALMENTE DAI SITI DI RICERCA PERSONE PIÙ RISCHIOSI

Inizia facendo manualmente l'opt-out dai siti più rischiosi:

1. **Fai l'opt-out da People Connect (Intelius)** - Possiedono un sacco di siti di ricerca persone, quindi un solo opt-out fa tanta strada. Compila il "suppression form", cioè il modulo di rimozione. Ti verrà chiesto di verificare la tua email o il tuo numero di telefono.
    - Se il sito ti chiede di verificare un numero di telefono o un'email a cui non hai accesso, chiama il loro supporto tecnico al (877) 564-3253 e chiedi di far rimuovere le tue informazioni personali, in inglese: "personal information suppressed". Per esperienza, chiamare funziona molto meglio che scrivergli un'email.
2. **Cercati su National Public Data.** Se trovi un risultato, scorri fino in fondo alla pagina e clicca su Do Not Sell My Info per fare l'opt-out.

Ci sono altri siti che troverai solo cercando manualmente le tue informazioni su Google (lo spieghiamo in una voce successiva della checklist).

Tutto a mano: se vuoi fare tutti gli opt-out manualmente, puoi usare la Big Ass Data Broker Opt-Out List di Yael Grauer. Servizi come EasyOptOuts gestiscono la maggior parte di questi siti al posto tuo, ma non tutti. Puoi usare questa lista per fare tutto a mano gratis, oppure per cercare manualmente in ogni database e vedere cosa ti è sfuggito.

☐ Chiedi la rimozione dai siti di "ricerca facciale"

Evita che una tua foto venga usata per risalire alla tua identità.

Puoi proteggerti chiedendo la rimozione dai siti di "ricerca inversa delle immagini". Così diventa più difficile usare la tua foto profilo online per scoprire il tuo nome legale, che potrebbe portare qualcuno a trovarti sui siti di ricerca di persone di cui abbiamo parlato sopra.

COME FARTI RIMUOVERE DAI SITI DI "RICERCA FACCIALE"

Ognuno di questi siti ti chiederà (ironia della sorte) di caricare una foto del tuo viso. È un male necessario se vuoi essere rimossə. Sta a te decidere se il rischio di dargli altri dati vale il vantaggio di essere rimossə.

> **Nota sul caricamento del documento d'identità**: alcuni di questi siti sono pessimi e ti chiedono di caricare una foto del tuo documento d'identità o del passaporto, con le informazioni sensibili nascoste. Il modo più semplice è coprire con del nastro adesivo tutto il documento tranne il nome e la foto, e poi scattare una foto.

Siti da cui chiedere la rimozione:

1. Rimozione da Clearview.ai - Serve solo una foto, non un documento d'identità. Purtroppo, l'opt-out è possibile solo negli stati che hanno approvato leggi sulla privacy. ***Clearview è usato soprattutto dalla polizia e dagli sbirri, quindi è importante chiedere la rimozione.***
2. Rimozione da PimEyes - Serve una foto del tuo documento d'identità. (Copri il numero del documento!)
3. Rimozione da FaceCheck.ID - Invece di caricare un documento d'identità, puoi caricare un selfie in cui tocchi il mento con due dita. Inoltre, devi selezionare a mano le foto che vuoi far rimuovere.

☐ Attiva le notifiche di "Risultati che ti riguardano" di Google

Ti aiuta a ricevere notifiche sulle pagine che contengono i tuoi dati personali.

Google offre Risultati che ti riguardano, uno strumento che ti avvisa quando le tue informazioni private vengono diffuse online. Non è granché utile per far rimuovere quei risultati, ma ti fa capire quando devi trovare tu il modo di far togliere le informazioni.

COME ATTIVARE "RISULTATI CHE TI RIGUARDANO" DI GOOGLE

1. **Attiva "Risultati che ti riguardano" di Google**: inserisci il tuo nome completo (e qualsiasi altro nome che usi), indirizzi, numeri di telefono e indirizzi email.

   > **Attenzione:** NON inserire **pseudonimi** o **numeri di telefono usa e getta** che usi solo per l'attivismo e che sono già completamente separati dalla tua vera identità. Non vorrai certo che finiscano collegati tra loro nei sistemi di Google.

2. **Aspetta** che la prima scansione sia completata (qualche ora)
3. **Controlla i risultati e trova il modo di farli rimuovere:**
   1. Usare il pulsante "richiedi rimozione" nello strumento di Google di solito non serve a molto, per due motivi: 1) Google rifiuta la maggior parte delle richieste, a meno che non riguardino un sito di "ricerca persone" o un caso di doxxing intenzionale. E 2) anche se Google le rimuove, le informazioni originali restano comunque in rete. Chiunque può trovarle su altri motori di ricerca o direttamente sul sito originale.
   2. Conviene invece provare a contattare chi gestisce il sito per far rimuovere le informazioni. Sui siti web, vuol dire trovare un modulo di contatto o un indirizzo email e segnalare la pagina che contiene le informazioni che vuoi far rimuovere. Sui social, può voler dire cancellare un post che hai pubblicato tu o chiedere a chi l'ha scritto di toglierlo.
   3. Clicca su "segna come esaminato" man mano che gestisci ogni elemento.
4. **Invia una "richiesta di rimozione" a Google:** usa questo modulo di richiesta di rimozione per chiedere a Google di rimuovere i risultati di ricerca che contengono i tuoi dati personali o altri contenuti di doxxing. È una cosa diversa dalla funzione "Risultati che ti riguardano" di Google.
5. **Tieni d'occhio le email di notifica** sui nuovi risultati man mano che compaiono. Di solito ne arrivano di più nelle prime due settimane dopo l'iscrizione.

Privacy: richiede un account Google. C'è un compromesso da considerare: stai dando a Google altri identificativi, come i tuoi altri nomi, numeri di telefono e indirizzi, che poi resteranno archiviati e collegati al tuo account. Di solito ne vale la pena, perché Google ha già la maggior parte di queste informazioni su di te, e il vantaggio è ricevere una notifica quando il tuo indirizzo o altri dati privati spuntano da qualche nuova parte sul web.

Blinda le impostazioni privacy dei tuoi account social

Quasi tuttə abbiamo condiviso molte più informazioni su di noi sui social prima di iniziare a voler proteggere la nostra privacy.

Blindare i nostri profili social può richiedere parecchio tempo.

Cose che potresti voler proteggere: la tua posizione, il tuo indirizzo email (può essere usato per cercarti anche se è nascosto), la tua lista di amicə, il tuo posto di lavoro, la tua data di nascita completa (può essere usata per accedere ad altri account, come quello della banca) e le foto/i post che mostrano dove passiamo più spesso il nostro tempo.

Esporsi pubblicamente o restare in privato: alcune persone hanno profili volutamente pubblici, con un seguito che vogliono mantenere perché li usano per il loro attivismo e la loro organizzazione politica. Per esempio, alcune persone potrebbero scegliere di lasciare i propri profili accessibili, mentre altre potrebbero scegliere di nasconderli, così che solo lə amicə possano vederli.

OPZIONE 1: COME BLINDARE LE IMPOSTAZIONI PRIVACY DEI TUOI SOCIAL CON BLOCK PARTY

Anche se puoi farlo a mano (vedi sotto), ti consigliamo di usare Block Party perché ti guida passo passo su quali impostazioni privacy cambiare. Ti aiuta a blindare Facebook, LinkedIn, Instagram, X/Twitter, TikTok, Snapchat, Reddit, Strava, Venmo, Google, le recensioni di Google Maps, YouTube e Bluesky. La versione gratuita è utile, e abbiamo letto la loro informativa sulla privacy: in generale ci fidiamo di chi l'ha creata.

1. **Installa l'estensione Block Party** (gratuita) sul tuo browser. (È il momento perfetto per installare Brave, se non l'hai ancora fatto!) Segui le istruzioni di installazione.
2. **Premi "Start Scan"** e seleziona i social che usi. Lascialo andare per qualche minuto mentre controlla tutte le tue impostazioni.
3. **Accanto a ogni sito, clicca su "To Do"** per vedere le modifiche consigliate. Puoi iniziare a farle a mano oppure lasciare che Block Party ne automatizzi molte.
4. **Puoi automatizzare molte delle modifiche:** Block Party farà in automatico per te il 50-70% delle modifiche alle impostazioni. Per questo serve una prova gratuita di 7 giorni o un account a pagamento (50 $/anno se usi il codice promozionale JOINTHEPARTY — non prendiamo nessuna commissione).
5. **Fai a mano le modifiche rimanenti:** segui le liste "To Do" di ogni sito per le modifiche che non si possono fare in automatico.
6. Infine, pensa a quali altri social o siti usi che potrebbero non essere coperti da Block Party: Cash App, Venmo (se non è già coperto), Partiful, Nextdoor, AllTrails, Strava, Pinterest, Goodreads, MapMyRun, app di incontri, ecc.

Se vuoi cancellare i tuoi vecchi post su X/Twitter o passare a Bluesky, dai un'occhiata a Cyd.

OPZIONE 2: COME BLINDARE A MANO LE IMPOSTAZIONI PRIVACY DEI TUOI SOCIAL

Se non vuoi usare Block Party, puoi seguire questi passaggi per ciascuno dei tuoi principali account social.

Siti a cui potresti voler dare la priorità (più o meno in ordine di rischio):

- Facebook
- LinkedIn
- Venmo
- Cash App
- Recensioni di Google Maps
- Yelp
- Strava
- All Trails
- Instagram
- X/Twitter *(Per cancellare i tuoi vecchi post, dai un'occhiata a Cyd.)*
- Bluesky
- YouTube
- TikTok
- Snapchat
- Reddit
- Partiful
- Nextdoor

Passaggi per ogni sito:

1. **Valuta se eliminare questo profilo** se non ti serve più. Molti siti (Facebook, Instagram, Google) ti permettono di scaricare prima una copia dei tuoi dati, così non perdi foto o messaggi. Se lo elimini, hai finito. Altrimenti, vai avanti.
    - **Ti serve solo Facebook Marketplace?** Valuta di creare un account Facebook secondario e fittizio da usare solo per Marketplace, e poi elimina quello principale.
2. **Trova la schermata delle impostazioni della privacy** e imposta tutto nel modo più privato possibile.
3. **Togli la tua città**
4. **Nascondi la lista dei tuoi contatti**
5. **Fai pulizia tra follower e contatti.** Rimuovi le persone che non hanno almeno una o due amicizie in comune con te, soprattutto se non le conosci davvero. Anche con un profilo "privato", chiunque tu abbia accettato come follower può comunque vedere i tuoi post e farne uno screenshot.
6. **Cancella vecchi post e foto** che rivelano dettagli su dove vivi, dove passi il tuo tempo e con chi.

Prova a usare Digital Footprint Check con i nomi utente che usi più spesso, per scoprire dove potresti avere profili di cui ti sei dimenticatə.

☐ Indossa una mascherina quando hai a che fare con gli sbirri o con avversari di destra

Ti aiuta a proteggerti se qualcuno con cattive intenzioni prova a usare il tuo volto per scoprire chi sei

La polizia e l'ICE usano il riconoscimento facciale contro chi dissente.

Gli avversari di destra spesso fotografano chi manifesta per fare ricerche inverse di immagini e identificare chi partecipa: alcuni gestiscono database come Canary Mission con profili di attiviste e attivisti. Coprire una parte o tutto il volto rende la cosa più difficile.

Una mascherina KN95 può aiutarti a sfuggire agli strumenti di riconoscimento facciale. Non è perfetta (ad alcuni strumenti bastano i tuoi occhi), ma aiuta parecchio.

Contano anche altri tratti riconoscibili. Coprirsi il volto non basta se altre parti di te sono facili da riconoscere. Gli avversari spesso identificano chi manifesta col volto coperto grazie a tatuaggi particolari, colore o taglio dei capelli, corporatura, colore della pelle e vestiti, soprattutto quando più di questi elementi si combinano. Valuta di coprire i tatuaggi visibili con le maniche lunghe, di indossare un cappello o un cappuccio e di cambiare i vestiti che usi alle proteste, se vuoi essere più difficile da seguire da un'azione all'altra.

> Come per altri punti di questa lista, privacy e visibilità possono essere in conflitto: c'è chi preferisce ridurre il rischio coprendosi volto e occhi, e chi invece preferisce mostrare il viso per intero per creare fiducia ed esprimere le emozioni in modo più diretto.

Nota legale: alcune città hanno approvato leggi anti-maschera che rendono illegale coprirsi il volto. Ti conviene controllare le ordinanze della tua città.

Completa la nostra checklist Fondamenti di sicurezza digitale

Questa guida tratta altri passaggi importanti per proteggerti dal doxxing, come password, permessi di localizzazione delle app e aggiornamenti software.

Se ti preoccupa il doxxing, è una buona idea completare i passaggi descritti nella nostra checklist Fondamenti di sicurezza digitale →

Molti di questi ti proteggeranno da chi cerca di accedere ai tuoi account o dispositivi se sei bersaglio di doxxing.

Questi punti della checklist Fondamenti sono particolarmente importanti:

- **Disattiva la localizzazione** per la maggior parte delle app
- **Installa gli ultimi aggiornamenti software** su laptop, telefono e app
- Usa un **password manager**
- **Cambia le password che usi già** se sono deboli o se le riutilizzi su più siti.
- Attiva l'**autenticazione a due fattori** sui tuoi account importanti
- Non cliccare su **link sospetti**

Non usare il tuo vero nome o una tua foto nel profilo Signal

Ti aiuta a proteggerti dagli sbirri o da chi vuole scoprire chi sei. Particolarmente utile se fai parte di gruppi Signal non verificati.

Molta organizzazione dal basso avviene in gruppi Signal non verificati, dove non sai quanto puoi fidarti di tutte le persone del gruppo. Questi gruppi possono essere infiltrati da avversari di destra e dagli sbirri.

Usare un nome falso impedisce che qualcuno risalga alla tua vera identità con una semplice ricerca su Google.

Usare una foto che non mostra il tuo volto impedisce che qualcuno trovi i tuoi profili social tramite la corrispondenza delle immagini o il riconoscimento facciale.

Entrambi i passaggi ti aiutano a difenderti dal doxxing e dalle molestie online.

COME MODIFICARE IL TUO PROFILO

1. **Cambia il nome visualizzato nel profilo:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → Tocca il tuo nome/icona in alto → Tocca la prima voce con la sagoma di una persona → Modifica il nome visualizzato nel profilo
2. **Cambia la foto del profilo:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → Tocca il tuo nome/icona in alto → **Modifica foto** → carica una foto generica trovata online che non abbia legami con la tua identità, i tuoi gusti, i tuoi interessi o il luogo in cui vivi.

Lo stesso principio vale ancora di più per i social media. Se il tuo profilo Instagram, Facebook o LinkedIn associa il tuo nome completo reale a una foto chiara del tuo volto, chi vuole attaccarti può identificarti facilmente anche se il resto del profilo è privato. Per saperne di più, vedi Blinda i tuoi social media.

Ricorda anche alle persone dei tuoi gruppi di fare queste cose. La sicurezza è un gioco di squadra.

Protezioni avanzate

RISCHIO MEDIO Questa sezione fa per te se hai un ruolo visibile legato al tuo dissenso politico.

☐ Configura Signal in modo che nessuno possa trovarti tramite il tuo numero di telefono

Anche se di default il tuo numero di telefono non è visibile su Signal, chiunque può comunque digitarlo e trovarti. Se rischi di subire molestie, potresti preferire condividere con le persone solo il tuo nome utente di Signal.

COME IMPEDIRE CHE TI TROVINO TRAMITE IL TUO NUMERO DI TELEFONO SU SIGNAL

1. **Se vuoi cambiare il tuo nome utente:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → Tocca il tuo nome/icona in alto → Tocca il simbolo **@** → **Modifica nome utente** → imposta un nome utente **completamente scollegato** dalla tua identità e da qualsiasi nome utente che hai già usato altrove. Deve finire con almeno 2 numeri.
2. **Nascondi il tuo numero di telefono:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Privacy** → **Numero di telefono** → In **Chi può vedere il mio numero** → Seleziona **Nessuno**.
3. **Impedisci che ti trovino tramite il tuo numero di telefono:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Privacy** → **Numero di telefono** → Sotto **Chi può trovarmi tramite il numero** → Seleziona **Nessuno**.
4. Quando vuoi metterti in contatto con qualcuno su Signal, dai il tuo nome utente invece del tuo numero di telefono.

☐ Procurati un numero di telefono alternativo invece di condividere pubblicamente il tuo numero principale

Il tuo numero di telefono può essere un modo rapido per trovare il tuo indirizzo di casa tramite i siti di "ricerca persone".

DO: Usa Google Voice (gratis, meno privato) o MySudo (2 $/mese, più privato)

DO NOT: Condividere il tuo numero di telefono pubblicamente online o in spazi grandi e non verificati

Condividere pubblicamente il tuo numero di telefono principale non ti espone solo a chiamate e messaggi molesti: se qualche sito di "ricerca persone" non ti ha ancora rimosso, chiunque potrebbe usare il tuo numero per trovare il tuo indirizzo di casa.

COME CONFIGURARE NUMERI DI TELEFONO ALTERNATIVI

- **Procurati un numero di telefono alternativo** se devi condividere un numero pubblicamente.
  - Google Voice è gratis, ma Google è il primo posto dove gli sbirri vanno a chiedere informazioni con un mandato, quindi è l'opzione meno privata.
  - MySudo costa 2 $ al mese per 100 messaggi e 30 minuti di chiamate.
  - Sideline (15 $/mese) o Line2 (10 $/mese) se ti servono messaggi/chiamate illimitati
- **Quando vuoi che le persone ti contattino su Signal, dai loro il tuo nome utente Signal** invece del tuo numero di telefono. (Ovviamente, usa Signal ogni volta che puoi, soprattutto quando ti organizzi. E ricordati di attivare i messaggi effimeri come impostazione predefinita nelle impostazioni.)

Chiedi alle persone con cui vivi di cancellare i propri dati personali dai siti di "ricerca persone"

Se vuoi che il tuo indirizzo resti privato, tutte le persone che vivono in casa con te devono proteggere i propri dati.

Uno dei nostri obiettivi principali è proteggere il tuo indirizzo di casa da malintenzionati.

Chi ti attacca, se è determinato, potrebbe scoprire con chi vivi attraverso i post sui social, le liste di amici o i siti di alberi genealogici. Se ti sei fatto cancellare dai siti di ricerca persone ma le persone con cui vivi o i tuoi familiari no, chi ti attacca potrebbe comunque riuscire a trovare il tuo indirizzo di casa.

I familiari che hanno il tuo stesso cognome sono un collegamento particolarmente forte, perché chi ti attacca può partire da uno qualsiasi di loro e arrivare dritto al vostro indirizzo comune sui siti di "ricerca persone".

COME AIUTARE LE PERSONE CON CUI VIVI A RIMUOVERE I PROPRI DATI PERSONALI

1. **Chiedi a ogni persona** con cui vivi di rimuovere i propri dati personali dai siti di "ricerca persone". Esempio di testo/messaggio:

   > Sto cercando di rimuovere da internet il nostro indirizzo di casa e gli altri miei dati personali, così siamo più protetti. Puoi prenderti qualche minuto per fare le prime due cose di questa checklist, così il nostro indirizzo non è facile da trovare online? https://activistchecklist.org/doxxing> Se questa settimana hai tempo, lo facciamo volentieri insieme.

2. Se può aiutare, puoi cercare il tuo indirizzo su Google e trovare le pagine specifiche in cui il loro nome è collegato all'indirizzo. Puoi mandargli il link a questa pagina per spiegare perché è importante. La maggior parte delle persone si sorprende di quanto sia facile trovare informazioni del genere online.
3. **Imposta un promemoria** per risentirli tra una settimana circa e vedere se hanno bisogno di una mano.

Potresti fare la stessa richiesta anche alle persone che vivevano con te al tuo indirizzo attuale, perché il loro vecchio indirizzo compare ancora sui siti di "ricerca persone".

Cerca a mano su Google le tue informazioni private

Ci saranno sempre risultati che dovrai trovare e rimuovere a mano.

Se ti affidi solo a strumenti di rimozione automatica dei dati come EasyOptOuts, probabilmente ci saranno comunque un sacco di risultati che mostrano le tue informazioni private.

La priorità è rimuovere il tuo indirizzo di casa attuale e, in secondo luogo, il tuo numero di telefono. La tua email potrebbe essere pubblica e portare a molestie, ma è più facile da gestire.

L'app Kanary (versione gratuita) può aiutarti a fare parte di queste ricerche.

COME TROVARE E RIMUOVERE LE TUE INFORMAZIONI PERSONALI SU GOOGLE

1. **Fai ricerche separate su Google per le tue informazioni.** Metti la ricerca tra virgolette per risultati più precisi. Scorri le prime 2–3 pagine di Google per ogni ricerca (per questo lavoro non usare Brave Search o altri motori di ricerca orientati alla privacy).
   - **Indirizzo di casa tra virgolette:** `"742 Evergreen Terrace, Springfield"` o anche solo `"742 Evergreen Tr"`, anche se così potrebbero uscire troppi risultati che non riguardano la tua città.
   - **Numero di telefono tra virgolette:** `"555-867-5309"` oppure `"5558675309"` oppure `"(555) 867-5309"`
   - **Nome completo più città (ciascuno tra virgolette separate):** `"Jamie Garcia" "Springfield"`
   - **Solo il tuo nome completo tra virgolette:** `"Jamie Garcia"` (darà un sacco di risultati che potrebbero non riguardarti)
2. **Tieni una lista** di quello che trovi che contiene le tue informazioni private sensibili. Dai la priorità ai siti che mostrano il tuo indirizzo o numero di telefono.
3. **Fai un piano per far rimuovere ciascun risultato.**
   - Se è un sito di "ricerca persone", cerca un modulo tipo "non vendere i miei dati" o "opt out" da compilare.
   - Se è un social, deve rimuoverlo chi l'ha pubblicato. Oppure, se non vogliono rimuoverlo, puoi provare a cliccare su "segnala contenuto".
   - Se è un altro tipo di sito, cerca un modulo di contatto e chiedi di rimuoverlo perché temi di diventare bersaglio di attacchi online. La maggior parte dei siti è disposta ad aiutare.
   - **Chiedi ai motori di ricerca di rimuovere il risultato.** In caso di molestie, doxxing o altri contenuti dannosi, puoi inviare una richiesta di rimozione direttamente a Google (modulo) e a Bing (modulo). Non sempre funziona, ma per i risultati più dannosi vale la pena provarci.
4. **Imposta un promemoria per ricontrollare.** Ricontrolla dopo una settimana. Se qualcuno di questi siti non ti ha risposto, prova a sollecitarlo.
5. **Imposta Google Alert** per ciascuna delle ricerche qui sopra, così ricevi una notifica quando escono nuovi risultati. (La funzione "Risultati che ti riguardano" di Google è utile, ma di sicuro qualcosa le sfugge.)
6. **Aggiorna i risultati di Google.** Se sei riuscitə a far rimuovere una voce dal sito di origine, ma compare ancora nei risultati di Google, puoi chiedere che il contenuto venga aggiornato.
7. **Prova anche altri motori di ricerca.** Ogni motore di ricerca mostra risultati diversi, e chi ti attacca non si limita a Google. Fai le stesse ricerche su Bing e DuckDuckGo per vedere cos'altro salta fuori.

☐ Blocca i tuoi report di credito

Ti protegge da chi prova ad aprire carte di credito a tuo nome.

Qualche malintenzionato potrebbe provare ad aprire carte di credito a tuo nome, danneggiando il tuo punteggio di credito e creandoti problemi economici a lungo termine.

Bloccare il tuo report di credito impedisce a chiunque di aprire carte o prestiti a tuo nome. Puoi sbloccarlo temporaneamente quando ti serve.

COME BLOCCARE IL TUO REPORT DI CREDITO

Devi attivare manualmente un "freeze" (blocco) presso **tutte e tre** le agenzie di credito:

- **Equifax**
- **Experian**
- **TransUnion**

È sempre gratuito. Non accettare nessuna delle offerte a pagamento che ti propongono.

In futuro, ricordati di sospendere temporaneamente il blocco quando dovrai far controllare il tuo report di credito per aprire un nuovo conto.

Sfoca la tua casa su Google Maps e Apple Maps

Così è più difficile per chi vuole farti del male capire com'è fatta la tua casa o il tuo cortile.

Se qualcuno con cattive intenzioni riesce a scoprire il tuo indirizzo, potrebbe cercare la tua casa su Google Maps per molestarti o farti del male di persona. Oppure potrebbe scoprire cose come il tipo di auto parcheggiata nel tuo vialetto.

COME SFOCARE LA TUA CASA SUI SITI DI MAPPE

Nota: una volta richiesta la sfocatura, non puoi più annullarla. Per la maggior parte delle persone, avere la propria casa visibile su Street View porta pochissimi vantaggi.

Sfoca la tua casa su Google Maps (dettagli):

1. Trova la tua casa su Google Maps.
2. Apri l'immagine di Street View che vuoi sfocare.
3. In basso a destra, clicca su “Segnala un problema” e compila il modulo indicando che vuoi sfocare la tua casa per motivi di privacy.

Sfoca la tua casa su Apple Maps:

1. Scrivi un'email a mapsimagecollection@apple.com. Indica il tuo indirizzo di casa e spiega che vorresti sfocarla per motivi di privacy.

Togli la tua casa dai siti immobiliari (Zillow, Redfin, ecc.)

Nascondere le foto dell'interno di casa tua aiuta a tenere tutte le persone più al sicuro.

Zillow, Redfin, Realtor.com e altri siti spesso non mostrano solo l'esterno di casa tua (che già comporta qualche rischio), ma possono mostrare anche una planimetria dettagliata dell'interno. Questo può dare a chi ti è ostile informazioni utili per molestarti o farti del male.

Puoi proteggerti chiedendo che le immagini relative al tuo indirizzo vengano rimosse.

COME RIMUOVERE LE IMMAGINI DI CASA TUA DAI SITI IMMOBILIARI

Se la casa non è tua, potresti dover chiedere a chi te l'affitta di fare queste rimozioni, perché serve un account su ogni sito. Deve "rivendicare" la casa su ciascun sito immobiliare.

Puoi anche cercare prima sul sito per vedere quanto sono dettagliate le foto e decidere se vuoi farle rimuovere.

1. Rimuovi da Zillow
2. Rimuovi da Redfin
3. **Realtor.com**: Log in → **Claim Home** → **Edit Photos**
4. Chiedi al tuo agente immobiliare di rimuovere le foto dall'MLS, il database condiviso degli annunci immobiliari negli USA, così spariranno anche da tutti gli altri siti.

Attiva la Modalità di isolamento (iPhone) o la Protezione avanzata (Google e Android)

Lo spyware è un tipo di attacco avanzato, che sfrutta vulnerabilità sofisticate dei nostri dispositivi. Per questo, Apple e Google hanno introdotto una modalità di sicurezza avanzata che offre una protezione più forte contro lo spyware.

Su iPhone si chiama **Lockdown Mode**, mentre su Android si chiama **Advanced Protection Program**. (Puoi attivare il Programma di protezione avanzata anche solo sul tuo account Google, pure se non hai un telefono Android.)

Non ci risulta nessun caso di persone infettate da spyware che avessero attiva la Modalità di isolamento di Apple. La Protezione avanzata di Android è più recente e la sua efficacia deve ancora essere messa alla prova.

Compromessi sull'usabilità: entrambe le funzioni comportano la rinuncia ad alcune funzionalità. Guarda l'elenco completo dei compromessi. Se incontri problemi che non vanno bene per le tue esigenze, puoi sempre disattivare la funzione più avanti.

COME ATTIVARE LA MODALITÀ DI ISOLAMENTO SU IPHONE

IPHONE

Impostazioni → **Privacy e sicurezza** → **Modalità di isolamento** → **Attiva la modalità di isolamento**

Questa funzione è disponibile da iOS 16 in poi.

COME ATTIVARE LA PROTEZIONE AVANZATA SU ANDROID

ANDROID

Impostazioni → **Sicurezza e privacy** → in **Altre impostazioni** tocca **Protezione avanzata**

Nota: la posizione di questa impostazione può cambiare da un dispositivo Android all'altro, quindi ti consigliamo di cercare 'Protezione avanzata' nella barra di ricerca delle Impostazioni.

Questa funzione è disponibile da Android 16 in poi.

Attiva il PIN di Signal e il blocco registrazione

Ti protegge da attacchi avanzati in cui qualcuno "ruba" il tuo numero di telefono e lo registra su Signal

Se qualcuno molto determinato riesce a scoprire il tuo numero di telefono, può provare a impossessarsene con una tecnica chiamata "SIM Swapping" oppure chiamando il tuo operatore e avviando la "portabilità" del numero verso un nuovo operatore. Poi potrebbero usare il tuo numero per registrare un account Signal e iniziare a ricevere i messaggi destinati a te.

Sono attacchi avanzati che alla maggior parte delle persone non capitano. Comunque, proteggere il tuo account Signal è facile.

Puoi proteggerti attivando il **blocco registrazione** su Signal. Impedisce a chiunque di prendere il controllo del tuo account, anche se riesce a rubarti il numero di telefono. Nessuno potrà registrare un nuovo account Signal con il tuo numero finché il tuo account non sarà rimasto inattivo per 7 giorni.

Se dimentichi il PIN, dovrai aspettare 7 giorni prima di poter creare un nuovo account (e i tuoi contatti non verranno recuperati). Scopri di più su PIN e blocco registrazione.

COME ATTIVARE IL PIN DI SIGNAL E IL BLOCCO REGISTRAZIONE

Attiva il blocco registrazione: Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Account** → Attiva **Blocco registrazione**

Rafforza il tuo PIN: hai dovuto impostare un PIN di Signal durante la configurazione. Se non te lo ricordi o vuoi usare un PIN più robusto, ecco come fare:

1. **Genera un PIN robusto:** per la massima sicurezza, usa un PIN di 8 o 10 cifre e assicurati che sia generato da un computer. Ecco un generatore di PIN casuali che puoi usare.
2. **Imposta un PIN di Signal:** Apri Signal → Tocca la tua immagine del profilo → **Impostazioni** → **Account** → **Crea/Modifica PIN** (se non sai già qual è il tuo PIN).
3. **Salva il PIN o attiva i promemoria del PIN:** se usi regolarmente un password manager, salva lì il tuo PIN. Se pensi di poter dimenticare dove hai salvato il PIN, lascia attivi i "Promemoria PIN".

Protezioni per chi è molto espostə

RISCHIO ALTO Questa sezione fa per te se potresti finire sotto i riflettori dei media per il tuo dissenso o se chi ti è ostile ha molte risorse.

☐ Investi in servizi avanzati di rimozione dei dati (es: Optery Ultimate)

Se rischi seriamente di essere attaccatə per le tue idee politiche, assicurati di aver fatto un lavoro accurato per ripulire i tuoi dati online.

Inizia passando dallo strumento automatico di rimozione dei dati EasyOptOuts a qualcosa come Optery Ultimate (250 $/anno). È tra gli strumenti automatici di opt-out più completi. Puoi anche valutare il piano Kanary Pro (10 $/mese) per una copertura in più.

A seconda del tuo livello di rischio, potrebbe valere la pena investire in un servizio di fascia alta che ripulisca a fondo i tuoi dati al posto tuo.

Servizi vicini al mondo attivista per la pulizia dei dati e la risposta al doxxing:

- Brightlines
- Convocation Research & Design

Puoi anche dare un'occhiata alla Access Now Helpline, che di solito è gratuita, ma molto più lenta e meno accurata.

☐ Fai una pulizia avanzata dei tuoi social e blinda tutto

I passaggi di base per blindare i social qui sopra sono un buon inizio. Se rischi seriamente di finire nel mirino, ti conviene fare una pulizia più approfondita.

COME FARE UNA PULIZIA APPROFONDITA DEI SOCIAL E BLINDARE TUTTO

1. Fai una lista di tutti i siti dove hai o hai avuto un profilo, anche quelli che non usi da anni. Non pensare solo alle grandi piattaforme: app di incontri, app per il fitness, siti di recensioni, app di pagamento e vecchi forum contano tutti.
2. Cerca i nomi utente che usi più spesso su Digital Footprint Checker e Instant Username per trovare profili che avevi dimenticato. Aggiungili alla tua lista.
3. Scorri la lista e segui questi passaggi per ogni sito:
   - Elimina il profilo se non ti serve più
   - Cambia il nome visualizzato
   - Cambia il nome utente
   - Rimuovi la tua foto profilo
   - Togli la tua posizione dalla bio
   - Nascondi post e foto che potrebbero rivelare dove ti trovi
   - Nascondi la lista dei tuoi amici
   - Cambia il tuo indirizzo email (valuta DuckDuckGo Email Protection o il "trucco del più" di Gmail).
   - Modifica le impostazioni della privacy.
4. Potrebbero volerci molte ore per finire. Spunta ogni sito quando hai finito, così puoi riprendere da dove avevi lasciato.

Consiglio: se ti serve un nome visualizzato, un nome utente o una foto profilo casuali, puoi usare questo generatore di identità.

☐ Apri una casella postale così puoi smettere di dare in giro il tuo indirizzo di casa

DO: Apri una **casella postale PO box** o usa un servizio di inoltro/scansione della posta come **iPostal1**

DO NOT: Continuare a dare a chiunque il tuo indirizzo di casa

Potresti voler smettere di dare il tuo vero indirizzo quando ti registri a dei servizi, ti fai consegnare pacchi, ecc.

Opzioni:

- **Casella postale PO box con USPS**: lo svantaggio principale è che FedEx e UPS non consegnano alle caselle postali.
- **UPS Mailbox**: costa di più, ma accetta posta da USPS e FedEx e ti garantisce comunque più privacy.
- **iPostal1**: ti offre la scansione della posta + il ritiro di persona, e accetta anche consegne da tutti i corrieri (compresi FedEx e UPS), che non sempre consegnano alle caselle postali. C'è un rischio per la privacy se i loro sistemi vengono violati, o se ricevono un ordine del tribunale che li obbliga a consegnare i tuoi dati.

Nota: UPS Mailbox e qualsiasi servizio di "casella postale virtuale" come iPostal1 ti chiederanno un documento d'identità e di firmare un modulo (USPS Form 1583) che viene inviato a USPS.

☐ Usa un'identità diversa per ogni account online che crei (nome, email, nome utente, numero di telefono)

Invece di registrarti con il tuo vero nome/email/telefono/ecc., puoi iniziare a usare **identità casuali e diverse per ogni account**.

Così è più difficile per chi ti attacca (e per le aziende tech) collegare i tuoi account sui vari siti e mettere insieme un profilo con tutte queste informazioni.

COME USARE UN'IDENTITÀ DIVERSA PER OGNI ACCOUNT

Quando è possibile, fai in modo che ognuno di questi dati sia diverso per ogni sito:

- **Nome visualizzato:** usa questo generatore di identità casuali.
- **Nome utente:** usa questo generatore di identità o questo generatore di nomi utente.
- **Foto profilo:** lasciala vuota o usa questo generatore di identità. Se usi la stessa foto su tutti i siti, chi ti attacca può fare una "ricerca inversa per immagini" e trovare tutti i tuoi account.
- **Indirizzo email** - Usa un servizio di alias email come:
  - Qwacky per usare alias email @duck.com (gratis, estensione per Chrome/Firefox)
  - Proton Mail (gratis/a pagamento)
  - Addy.io (gratis/a pagamento)
- **Numero di telefono:** quando te lo chiedono, prova semplicemente a non inserirlo. Se devi inserire un numero di telefono solo per la verifica durante la registrazione, prova a noleggiarne uno da SMSPool (0,50 $ per registrazione). Se ti serve un numero di telefono a lungo termine, valuta MySudo.

☐ Aiuta le persone intorno a te a difendere le loro informazioni private (famiglia, amicə, colleghə, compagnə, vicinə di casa)

Se sei un bersaglio ad alto rischio, valuta quanto è probabile che anche altre persone della tua vita vengano prese di mira per molestarti o farti del male. Succede spessissimo quando unə attivista finisce in prima pagina. Troll e giustizieri di destra se la prenderanno con familiari, coinquilinə, amicə, colleghə, compagnə, vicinə di casa.

Scrivi alle persone della tua vita e suggerisci loro di fare almeno la prima sezione di questa guida.

Ecco il link alla checklist che stai guardando ora: https://activistchecklist.org/doxxing

A volte fare questi discorsi può essere difficile (soprattutto con la famiglia). Potrebbe volerci un po' di tempo per spiegare a qualcunə perché è a rischio a causa delle azioni che stai portando avanti tu.

Potresti anche voler avvisare in anticipo chi ti dà lavoro (e lə colleghə che gestiscono le comunicazioni, come la reception o le risorse umane) che sei a rischio di molestie, così capiscono la situazione se ricevono chiamate o email sospette o preoccupanti su di te.

☐ Prepara un piano di emergenza personale nel caso tu venga minacciatə a casa

Il livello più grave di attacco legato al doxxing è quando qualcuno ti trova di persona, a casa tua o in altri luoghi della tua vita, per molestarti, minacciarti o cercare di farti del male.

Segui la nostra Checklist per il piano di emergenza personale →

Queste sezioni della checklist sono particolarmente utili quando si parla di rischi legati al doxxing:

- Sezione 3: Sicurezza in casa
- Sezione 4: Piano di evacuazione

☐ Aggiungi un PIN di sicurezza ai tuoi conti bancari e al tuo account del telefono

I tuoi conti bancari e l'account del tuo operatore telefonico sono bersagli di grande valore, dove conviene aggiungere protezioni extra. Alcuni di questi servizi verificano la tua identità solo con il numero di telefono, l'indirizzo e/o la data di nascita. Sono tutte informazioni che chiunque potrebbe trovare online su di te.

Aggiungere un PIN o altre misure di sicurezza aiuta a garantire che solo tu possa accedere.

COME AGGIUNGERE UN PIN AGLI ACCOUNT SENSIBILI

Ecco alcuni degli account che conviene proteggere.

1. Conti bancari, carte di credito, prestiti, mutui e conti di investimento
2. Il tuo operatore telefonico (Verizon, T-Mobile, AT&T, ecc.)
3. Fornitore di internet
4. Fornitori di luce, gas e acqua
5. Assicurazioni (sanitaria, casa, auto, ecc.)

Come aggiungere un PIN a ogni account:

1. Chiama il loro servizio clienti.
2. Chiedi se puoi aggiungere un PIN di verifica.
3. Genera un PIN casuale per ogni account.
4. Salvalo nel tuo password manager.
5. Se non puoi aggiungere un PIN, chiedi quali altre misure di sicurezza offrono per impedire che qualcuno si spacci per te e acceda al tuo account.

Riepilogo degli strumenti

In questa guida segnaliamo tanti strumenti e abbiamo voluto raccoglierli in un unico posto:

- Funzione "Risultati che ti riguardano" di Google: ti avvisa quando le tue informazioni personali compaiono in un nuovo risultato su Google.
- EasyOptOuts (20 $/anno): rimuove i tuoi dati da tutti i siti di "ricerca persone".
- Block Party: ti guida passo passo nelle impostazioni da cambiare su ciascuno dei social più popolari.
- Cyd: ti aiuta a cancellare o fare il backup dei tuoi post su X/Twitter (e, se vuoi, a spostarli su Bluesky).
- Generatore di identità di StrongPhrase.net: ti aiuta ad avere nome, nome utente ecc. casuali da usare su ogni sito.
- MySudo o Google Voice: procurati un numero di telefono secondario, così non devi dare il tuo numero vero.
- Qwacky per usare le email @duck.com o Proton Mail o Addy.io: usa un servizio di alias email per generare un indirizzo diverso per ogni sito, così nessuno può collegarli tra loro.
- SMSPool: ti permette di noleggiare un numero di telefono casuale per pochi minuti, per ricevere l'SMS di verifica quando ti iscrivi a servizi che chiedono un numero di telefono.
- Optery (250 $/anno): per chi è esposto a minacce elevate. Fa la stessa cosa di EasyOptOuts, ma si spinge un po' più in là. (Spesso si consiglia DeleteMe, ma Optery è più efficace.)

Nota: gli strumenti ti aiutano fino a un certo punto, alcuni passaggi vanno fatti a mano.

Come reagire al doxxing e alle molestie online

Non abbiamo ancora una guida completa su come reagire al doxxing, ma vogliamo comunque darti qualche punto di partenza.

Come reagire al doxxing:

1. **Metti al primo posto la tua sicurezza fisica:** vai a casa di un'amica o un amico o in un posto sicuro se temi di rischiare danni o molestie imminenti. Fidati del tuo istinto. Meglio chiedere supporto e scoprire che non è successo niente che il contrario.
2. **Prenditi cura del tuo benessere emotivo:** anche molestie che sembrano "minori" possono essere molto stressanti, perché non sai se le minacce si concretizzeranno. Prenditi cura di te.
3. **Fatti aiutare:** non affrontarlo da solə. Fatti accompagnare da qualcuno in ogni passaggio.
   - Trova amicə/compagnə che ti sentano spesso e ti aiutino a mantenere i piedi per terra.
   - Chiedi supporto a chi se ne intende: Access Now 24/7 Helpline (gratuita), Equality Labs, Brightlines (a pagamento, fascia alta), Convocation Research & Design (a pagamento, fascia alta).
4. **Documenta tutto:** non cancellare niente e non bloccare nessuno. Può servire più avanti per risalire a chi c'è dietro gli attacchi. Se ne hai bisogno, affida questo compito a una persona di fiducia. Come documentare.
5. **Non chiamare gli sbirri:** potrebbero usare un'indagine per scoprire di più sulle reti attiviste. Detto questo, in alcune situazioni le leggi locali contro le molestie potrebbero tutelarti. Valuta di consultare un'avvocatə vicinə ai movimenti prima di rivolgerti allo Stato e/o coinvolgere gli sbirri nella tua situazione. Avvocatə vicinə ai movimenti a cui potresti rivolgerti: CLDC (linea di risposta rapida: 541-603-6891) o NLG.

Scopri di più su come reagire:

- Brightlines - Risorse sul doxxing
- Right To Be - Guida per rispondere al doxxing
- Right To Be - Guida alla cura di sé
- PEN America - Cosa fare se hai subito doxxing o sei finitə in una lista di sorveglianza
- PEN America - Online Harassment Field Manual - Rispondere al doxxing
- Crimethinc - Prevenzione e cura per chi è preso di mira da doxxing e molestie politiche (2020)

Continua a imparare con queste guide correlate

Piano di emergenza

Fai un piano nel caso in cui ti arrestino o ci siano minacce da parte degli avversari a casa tua.

Sicurezza su Signal

Tieni private le tue chat, anche se il telefono viene perso, sequestrato o compromesso.

Telefono secondario

Prepara un telefono in più per l'attivismo e le manifestazioni.

Protezione dallo spyware

Proteggiti dallo spyware e dai software di sorveglianza.

Pro e contro della Modalità di isolamento 3 min di lettura

Poster "Gli sbirri alla porta"