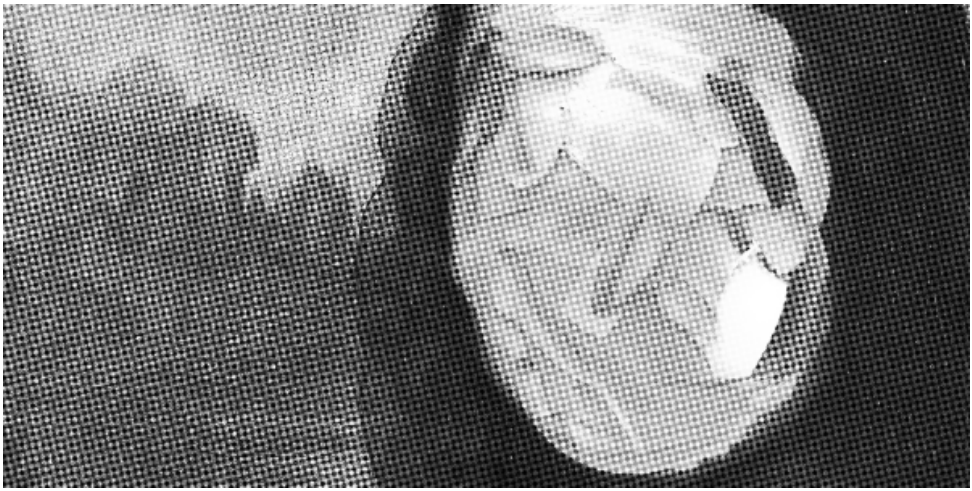
Doxcare

Prevenzione e follow-up per chi viene preso di mira da doxxing e persecuzioni politiche



Doxcare: Prevenzione e follow-up per chi viene preso di mira da doxxing e persecuzioni politiche

Original text in English

Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment

2020

crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment

Italian translation

it.crimethinc.com/2020/08/26/doxcare-prevenzione-e-follow-up-per-chi-viene-preso-di-mira-da-doxxing-e-persecuzioni-politiche

Layout

No Trace Project

notrace.how/resources/it/#doxcare

Questa guida dettagliata spiega come proteggersi dagli stalker online, perché è importante e cosa fare se si è presi di mira dal «doxxing», ovvero la pubblicazione delle proprie informazioni riservate. In un'epoca di sorveglianza universale, quando i livestreamer trasmettono tutte le principali manifestazioni mentre fascisti, agenti dell'FBI e agenti di Polizia setacciano i post sui social per raccogliere informazioni con cui perseguitare gli attivisti, non c'è mai stato un momento migliore per prendere provvedimenti per proteggere la tua privacy. Ecco come fare.

Contents

Introduzione: storia di una persona

«Da anni sono attivo nella mia comunità. Non molto tempo fa, i troll di estrema destra hanno trovato sui social gli account dei miei amici, della mia famiglia e del mio posto di lavoro. Mi hanno pedinato e hanno usato le foto mie e dei miei familiari per ricostruire le sequenze temporali della mia vita e per mappare i miei social network. A causa delle mie convinzioni antirazziste, hanno usato le informazioni raccolte per minacciare me, la mia famiglia e i miei amici. In ogni e-mail persecutoria e in ogni commento sui social, definiscono i progetti a cui partecipo come 'gruppi terroristici', descrivendomi come un 'leader' e un membro di una immaginaria 'folla ambigua di violenti individui di sinistra' per cui vogliono 'fare qualcosa di serio'. Che queste conclusioni siano solo un lavoro investigativo dozzinale o false dichiarazioni intenzionalmente disoneste, il loro comportamento dovrebbe preoccupare chiunque creda sia necessario resistere all'oppressione.

Quando ho saputo quel che stava accadendo, ho disattivato i miei social—non perché mi vergogni di essere associato alla lotta per un mondo più libero ma perché voglio proteggere i miei amici e i miei social. Chi mi conosce sa che non faccio mistero del fatto di oppormi a tutte le forme di fanatismo e oppressione. Non mi hanno preso di mira specificamente per qualcosa in particolare che ho fatto ma perché queste sono contrari a tutto l'attivismo anti-razzista, femminista e queer e pensano di poterci isolare e intimidire uno a uno. Questo è il motivo per cui dobbiamo sostenerci a vicenda.

Voglio che tu lo sappia nel caso ti capitasse di trovarti nella stessa situazione. Non sei solo. Spero che questo t'incoraggi a pensare seriamente alla tua sicurezza online personale e alla sicurezza dei tuoi familiari e amici.

Robert Bowers, lo stragista della sinagoga di Pittsburgh, ha chattato pubblicamente con troll dell'Alt Right (l'estrema destra americana) che hanno doxxato gli antirazzisti . La campagna di stalking attuata nei miei confronti mostra che sono disposti a fabbricare menzogne per mettere le persone al centro del mirino. L'unico modo per proteggerci è continuare a sostenerci a vicenda. Non dobbiamo lasciare che c'intimidiscano.»

Cos'è il doxxing?

Doxxing significa pubblicare le informazioni riservate di una persona con l'intenzione di esporla e intimidirla. Ciò può provocare danni fisici, emotivi

ed economici al bersaglio. Ha lo scopo di dissuadere il target dall'azione e di metterlo in imbarazzo per le sue idee e per i suoi valori. È importante prendere sul serio la sicurezza prima di essere doxxati—prima ancora di avere motivo di temere di poter esserlo. Un doxxer aspetterà spesso di aver raccolto molte informazioni prima di darle in pasto agli altri. È possibile che tu sia già stato stalkerizzato e non lo scoprirai fino a quando non sarà troppo tardi.

Che tu sia un noto attivista pubblico o che tu sia poco coinvolto, dovresti tenere al sicuro i tuoi social network e altri àmbiti della tua vita, anche se pensi di non far nulla che meriti attenzione. Mantenere buone pratiche protegge i tuoi amici, la tua famiglia e la tua comunità. È frequente che le persone siano incluse nelle teorie complottiste di destra sui «membri dell'Antifa» solo perché sono queer o trans, «sembrano di sinistra,» suonano in una band, partecipano a un evento o frequentano spazi radicali. Le informazioni non devono essere corrette o giustificate affinché tu sia preso di mira. Tutto ciò di cui un persecutore ha bisogno è un'informazione per iniziare a cercare maggiori dettagli online.

Essere consapevoli delle tracce che si lasciano online può proteggerti dalle forze dell'ordine e dagli stalker. Ora che la sorveglianza imposta dallo Stato è sempre più sofisticata e il live streaming è diventato normale durante le proteste, spesso non basta indossare una maschera. Nel giugno 2020 a Filadelfia, gli investigatori hanno identificato una donna iniziando con nient'altro che una sua foto sfocata. Hanno seguito una scia di briciole tra cui un acquisto su Etsy, un account Twitter e la sua pagina di lavoro. La Customs and Border Protection (Dogana e Polizia di Frontiera) ha iniziato a scandagliare i social media pubblici . Proteggere la tua presenza online può farti sentire più sicuro nell'agire offline.

Prevenire è meglio che curare

Non c'è momento migliore per iniziare di adesso. Dopo essere stato doxxato, potresti non essere in grado di eliminare le informazioni in circolazione, anche se dovessi provare a rimuoverle.

Ci sono molti modi diversi per affrontare questo problema. Ovviamente, il modo migliore per assicurarti che nessuno possa trovare informazioni

su di te è non avere nulla di disponibile ma alcune persone non possono eliminare la propria presenza online a causa del lavoro, della famiglia o di altre responsabilità. In alcuni casi, esistono ragioni strategiche per mantenere una sorta di identità online; per esempio, avere un account social di lunga data, credibile ma innocuo può essere utile per i non cittadini che attraversano il confine degli Stati Uniti . Per fortuna, ci sono modi per proteggere diversi àmbiti della tua vita, curare un profilo pubblico se ne hai bisogno e adottare pratiche che possono aiutare te e i tuoi amici a sentirvi autorizzati a continuare ad agire nella vostra comunità. Questo processo può essere noioso. Ci vorranno tempo ed energia. Consiglio di farlo insieme ad amici, coinquilini o familiari per avere assistenza in alcuni degli aspetti difficili o noiosi.

Mantenere àmbiti separati

Se non puoi cancellarti completamente dal Web, puoi comunque preservare una privacy relativa mantenendo àmbiti distinti[1] dell'attività online e ripulendo quegli account dimenticati o utilizzati di rado.

È probabile che tu abbia più di un'identità online. Ciò potrebbe includere social, piattaforme virtuali, siti di lavoro, account di posta elettronica, qualsiasi cosa a cui devi accedere. Spesso, nel doxxing, le informazioni vengono triangolate da molte fonti diverse. Un modo per ridurre la quantità d'informazioni disponibili per i doxxer è suddividere questi àmbiti in modo che non siano collegati tra loro. Questo processo è altamente individualizzato; prenditi un po' di tempo per considerare le seguenti domande e mappare i tuoi àmbiti online.

Trascorri il tuo tempo a discutere di politica o sulla bacheca di un conoscente di Facebook? Ti piacciono o riposti spesso gli stati di account radicali di Instagram o Twitter? Hai immagini o informazioni personali sulle bacheche di lavoro? Compri su Etsy o su eBay? Qualcuno dei tuoi amici pubblica foto tue sui loro account Instagram? Devi pubblicizzarvi online per il settore lavorativo in cui ti trovi? Ti colleghi con i tuoi colleghi,

[1] Il concetto di àmbiti è stato sviluppato dal Collettivo Smiling Faces.[a]

[a] https://smilingfacecollective.github.io/guide-to-preventing-doxxing

familiari e amici attivisti utilizzando lo stesso account? Usi parti del tuo vero nome o del tuo compleanno per nomi utente o e-mail?

Ognuno di questi fattori potrebbe non essere un problema in sé e per sé ma insieme possono creare collegamenti tra diverse àmbiti della tua vita.

Chiediti:

- Quanto sono separati ciascuno di questi account/identità?
- Cos'è pubblico? Cos'è privato?
- Cosa significano pubblico e privato nel contesto di ogni sito?
- Cosa si può trovare cercando il proprio nome completo?
- Usi lo stesso nome utente o e-mail per più account? Questi s'intersecano in àmbiti distinti della tua vita? Prenditi un attimo per pensare al modo in cui tutti questi àmbiti si sovrappongono offline.
- Il tuo lavoro ti permette di essere chiaro sulla tua inclinazione politica?
- Quanto è pubblico il tuo attivismo? Parli con i giornalisti? Lavori presso un infoshop ?
- Filtri alcuni o tutti i tuoi contenuti sui social dai parenti?
- Ci sono riferimenti ad attività illegali o controverse in un determinato profilo?

Di seguito sono riportati alcuni esempi di come la tua presenza online può sovrapporsi su diversi siti:

Parenti: Quanto è aperto il tuo rapporto con i tuoi consanguinei/parenti acquisiti? Se uno sconosciuto avesse informazioni su una sola persona in questa rete, cosa potrebbe scoprire sugli altri?

Politica: Discuti o pubblichi le tue convinzioni politiche online? In caso affermativo, su quali piattaforme?

Amici e comunità: Se hai dei social, chi sono i tuoi amici? I tuoi follower? In che modo le tue comunità online riflettono le tue comunità IRL?

Hobby: Quali sono i tuoi hobby? Hai amici e comunità grazie a loro? Fai parte di qualche comunità Internet dedicata a questi hobby?

Legale: Chi sei sulla carta? A quali nomi, numeri di telefono e indirizzi sei legato? Qualcuno dei tuoi account include queste informazioni? Ne esistono altri (probabilmente senza il tuo consenso)?

Carriera lavorativa: Il tuo lavoro prevede una presenza online, un sito Web o un account social? Ci sarebbero problemi se la tua attività politica si sovrapponesse alla tua carriera? O la tua carriera è in qualche modo legata alla tua identità politica?

Prenditi del tempo per considerare dove ti sovrapponi, quali sono i tuoi obiettivi online e dove puoi separare questi àmbiti.

Tattiche

Parliamo di come scoprire quali sono le informazioni disponibili su di te, come identificare ed eliminare le tracce e quali risorse online esistono per rimuoverle.

Inizia con ciò che è disponibile pubblicamente. Googlati e fai un elenco di tutti i tuoi account sui social. Eliminate i vecchi account per le cose che non usi più. Questo è anche un buon momento per scaricare un gestore di password come 1Password[2] e LastPass[3] che ti assista nella gestione di nomi utente, e-mail e password univoci.

Elimina siti Snoop/Data Broker

Scopri quali informazioni le persone possono trovare su di te utilizzando semplicemente un motore di ricerca. Cercati su DuckDuckGo e Google. Prova a eseguire questa ricerca in modalità di navigazione in incognito. Prova diverse versioni del tuo nome, con e senza il secondo nome e tra virgolette. Puoi impostare Google Alert per inviarti delle e-mail quando il tuo nome compare sul Web. Questo ti darà un'idea di quanti dati su di te sono disponibili online per le persone che non fanno parte della tua rete.

Dopo questa ricerca iniziale, dai un'occhiata a tutti i siti data broker che traggono profitto dal trading di dati personali. T'incoraggio anche a rimuovere i tuoi familiari più stretti allo stesso tempo. Questo processo può essere arduo; questi siti cercano di rendere il più difficile possibile l'eliminazione delle informazioni su di te. Ci sono alcune cose da cui non puoi rimuoverti, per esempio se ti siete registrato di recente per votare

[2]https://1password.com
[3]https://lastpass.com

e vivi ancora a quell'indirizzo (questo è un altro motivo per cui alcune persone scelgono di non votare).

Tra i siti host più sfruttati vi sono: Been-verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, OneRep e FamilyTreeNow. Ti consiglio di iniziare con questi, cercando ognuno su questo sito Web,[4] che ha una guida per rinunciare praticamente a tutti i data broker. Se hai più soldi che tempo, puoi pagare un servizio chiamato Delete Me[5] per rimuovere le tue informazioni ma, di solito, consiglio questo servizio solo se si è già stati derubati.

Elimina i vecchi account

Quando ti cerchi in un motore di ricerca online, potresti trovare anche vecchi account. Può essere utile fare una ricerca inversa usando tutti i vecchi nomi utente e i nickname che ricordi. Gli account che non usi da molto tempo possono renderti vulnerabile perché se usano una vecchia password, possono cercare di contattare il supporto tecnico di quell'account per ottenere ulteriori dati su di te e cercare di utilizzarli per altri account. Scarica tutto ciò che per te ha un valore sentimentale e chiudi definitivamente tutti gli account che non utilizzi più. Questi possono essere pieni d'indizi sulla tua vita.

Per prima cosa, vai su questo sito Web,[6] che ricerca su centinaia di piattaforme per nomi utente specifici, e cerca tutti i possibili nomi utente ed e-mail da te usati. Questo ti dirà quali piattaforme hanno account che utilizzano quella modalità.

Poi, vai qui[7] e digita il dominio del sito Web. Questo sito archivia una vasta gamma di siti Web esistenti, classifica quanto sia facile o difficile eliminare un account e fornisce il collegamento alla pagina «Elimina profilo» per ogni sito.

---

[4]https://joindeleteme.com/blog/opt-out-guides

[5]https://web.archive.org/web/20210804023430/https://onlinesos.org/blog/i-tried-abine-delete-me-to-get-my-info-off-data-broker-websites

[6]https://namechk.com

[7]https://backgroundchecks.org/justdeleteme

Il sito Web haveibeenpwned.com ti aiuterà a scoprire se ci sono violazioni dei dati che coinvolgono i tuoi account. In caso affermativo, intervieni immediatamente per modificare le password.

Modifica username, indirizzi e-mail e password

Il modo più semplice per cui qualcuno possa trovare ulteriori informazioni su di te è cercare il tuo nome, alias e username. Per mantenere separati i tuoi àmbiti di attività su Internet, utilizza *sempre* un nuovo nome utente quando crei un account. Se hai un sito professionale per lavoro e devi utilizzare il tuo nome completo, assicurati che l'e-mail utilizzata per quell'account sia utilizzata esclusivamente a tal scopo. Potrebbe essere necessario disporre di una manciata di account e-mail e username. Ne ho uno per tutti i miei account medici e governativi, uno per i miei acquisti online, uno per la mia vita politica e uno per i miei social, un altro per i siti d'incontri e così via. Utilizzo alias e false informazioni per tutti i siti Web che mi rappresentano o che visualizzano foto in cui compaio.

Un gestore di password è di grande aiuto per questo, poiché memorizzerà gli accessi per tutti i tuoi account. Consiglio LastPass che puoi scaricare per il uo telefono e per il browser. Potresti essere tentato di rimanere connesso in modo permanente ma assicurati sempre di disconnetterti quando hai finito di usarlo. Innanzitutto, per non dimenticare la password principale e anche per assicurarti che anche se qualcuno dovesse riuscire ad accedere al tuo telefono o PC, non potrebbe accedere a tutti i tuoi dati personali. Prenditi questo tempo per creare nuove e-mail e cambiare gli username per tutti gli account che non intendi eliminare. Puoi facilmente creare nuove e-mail usando Protonmail.[8] LastPass può aiutare a generare password di stringhe casuali, che sono le più sicure.

Scegli ciò che è disponibile e modificate le impostazioni sulla privacy

Dopo aver eliminato le questioni in sospeso, dai un'occhiata a ciò che hai scelto di conservare e a cosa puoi trovare lì. Se mantieni degli account sui social, controlla il tuo profilo e prendi nota di ciò che le persone possono scoprire su di te. Puoi scegliere tra una serie di strategie su come affrontare

[8]https://protonmail.com

questo problema, a seconda di quanto vuoi essere cauto e di quanto sei certo che sia possibile mantenere distinti i vostri diversi àmbiti di attività su Internet.

Alcune delle opzioni sono:

- Elimina tutte le foto in cui compari tu, i tuoi animali domestici, della tua auto, della tua casella di posta, dei tatuaggi e di qualsiasi altra cosa che includa dati identificativi non necessari, in particolare la tua immagine pubblica del profilo.
- Elimina o falsifica qualsiasi dato personale nel tuo profilo: fornisci un compleanno impreciso o nessun compleanno, scegli risposte casuali per la tua città natale, le scuole che hai frequentato e altre informazioni.
- Elimina follower e amici dubbi. Se modifichi tutte le impostazioni dei tuoi social in privato e ti senti sicuro della tua lista di follower, potrebbero esserci meno motivi per nascondere la tua faccia. Consiglio comunque di mantenere offline i dettagli sulla tua posizione e sulla tua vita personale. Ricorda, sei al sicuro solo come la persona più aperta della tua vita. Se scegli di essere più pubblico, tieni separati i tuoi amici e la tua famiglia, non pubblicare le loro foto o le loro informazioni personali senza il loro consenso informato e ricorda che le connessioni sociali sono visibili attraverso i social network e i siti di raccolta dati.

Il C.O.A.C.H[9] di Crash Override Network è un'utile guida dettagliata che ti collega direttamente alla pagina delle impostazioni sulla privacy per molti social network di uso comune. Clicca su «Let's Get Started» («Iniziamo») e «Strengthen the security of my online accounts so people can't break into them as easily» («Rafforza la sicurezza dei miei account online in modo che le persone non possano entrarvi facilmente») e segui le loro guide per tutte le principali società di social media. Questa guida può anche essere utile per altri aspetti della sicurezza online, quindi dopo averlo fatto, ti consiglio di chiudere il Coach helper e controllare quali altre risorse vengono offerte.

Quando pensi di aver finito, chiedi a un amico di provare a creare un profilo in base alle informazioni che possono essere trovate su di te mentre fingi

[9]https://crashoverridenetwork.com/coach.html

di essere un «doxxer» per vedere se qualcosa a cui non pensavi è passato inosservato. Potrebbe essere importante controllare periodicamente cos'è possibile trovare cercando il tuo nome ogni pochi mesi.

Se sei stato doxxato

Sconsigliamo di rivolgerti alla Polizia quando si è doxxati (o di non farlo mai). La Polizia può utilizzare le informazioni da te fornite sui persecutori ma utilizzerà anche quelle che ottengono su te e su altri individui e su gruppi cui potresti essere stato associatopubblicamente. Una volta archiviato, è definitivamente nelle loro mani e non è detto che non lo useranno per prendere di mira te o altri attraverso la repressione statale.

Se hai scelto di coinvolgere la Polizia, sia trasparente e non chiedere a nessun gruppo radicale di sostenerti. Assicurati di mettere al corrente della vostra decisione tutti i gruppi con cui sei connesso. Di solito, la Polizia non farà nulla o peggiorerà la situazione. L'idea di questa guida è di fornirti alternative basate sul sostegno della comunità e sull'empowerment.

Devo uscire allo scoperto?

Risposta breve: non reagire immediatamente in pubblico. Prenditi del tempo per metterti al sicuro e per avvisare le tue reti in privato prima di reagire pubblicamente.

Il tuo primo impulso potrebbe essere di avvisare immediatamente quante più persone possibile con un annuncio pubblico o di chiudere tutto. Uscire allo scoperto in questo modo può fornirti un supporto immediato se hai un pubblico comprensivo ma implica il rischio di una maggiore aggressività da parte dei persecutori. Ci sono buoni motivi per essere cauti con le informazioni all'inizio. La prima cosa più importante da fare è prendere provvedimenti per proteggere te stesso e le tue reti da ulteriori danni.

Dichiarazioni immediate possono complicare i tuoi tentativi di essere al sicuro. Indipendentemente dal fatto che le informazioni pubblicate su di te siano accurate o meno, è probabile che nessuno le utilizzi per causarti danni gravi senza prima averne confermate almeno una parte. Pubblicare su un account social la conferma di essere stato doxxato conferma immediatamente che le informazioni su di te sono accurate; indica anche

che hai visto dove è stato pubblicato e suggerisce che sei terrorizzato. Questo incoraggia i tuoi persecutori. Vogliono intimidirti e isolarti. Non confermare o non negare nessuna delle informazioni che hanno scoperto su di te, a prescindere dal fatto che siano false o imbarazzanti. Vogliono che tu reagisca. Se fai saper loro che ciò che hanno pubblicato non è corretto, potrebbero concludere di essere sulla strada giusta e che devono solo continuare a scavare. Qualche volta, una delle risposte pubbliche iniziali più efficaci è l'assenza di risposta: non modificare sostanzialmente le tue abitudini di pubblicazione e non mostrare alcun timore. Questo può trasmettere il messaggio che il tuo doxxer ha mancato il bersaglio e che l'attacco è stato un fallimentare.

Dopo aver avuto il tempo di elaborare quel che provi e aver messo in sicurezza la tua posizione, potrebbe essere strategico uscire allo scoperto e, forse, unirsi ad altre persone che si trovano in situazioni simili. Potresti essere in grado di sfruttare l'indignazione pubblica nei confronti dei suprematisti bianchi per creare una campagna per dissuadere ulteriori doxxing—per esempio, fare una raccolta fondi con l'impegno di donare del denaro per ogni e-mail persecutoria che tu o altri nella vostra comunità ricevete! Dal momento che i tuoi persecutori vogliono isolarti, un sostegno pubblico come questo potrebbe dissuaderli da intimidirti ulteriormente. Cerca di essere creativo, resiliente e strategico. Presta attenzione a non mettere in pericolo nessun altro in questo processo.

Quando rilasci delle dichiarazioni pubbliche, se ti dai delle arie o ti vanti delle tue capacità, della tua abilità di far ricorso alla violenza, ad armi con le quali puoi difenderti o amplifichi la tua ferocia, potresti fare il passo più lungo della gamba. In genere, non è una buona idea rappresentarti in modo falsato. Di solito, parlare direttamente o indirettamente con i persecutori non migliora le cose. Consiglio di fare una dichiarazione positiva facendo valere la tua etica e le tue convinzioni, descrivendo come la tua identità o i tuoi ideali ti hanno trasformato in un bersaglio sostenendo però che laddove queste campagne persecutorie hanno lo scopo di farti indietreggiare, non lo farai, perché non hai motivo per nascondere la tua inclinazione politica. Evita di parlare di azioni o di gruppi specifici, che tu ne sia coinvolto o meno.

Immediatamente dopo essere stato doxxato

1. **Niente panico.** Chiama un amico fidato che venga ad aiutarti.
2. **Crea un registro degli incidenti** e tienine traccia per le provocazioni online e offline. Questo è fondamentale per identificare i modelli degli attacchi. Può essere utile confrontarli con altri organizzatori per identificare schemi più ampi in modo da individuare i tuoi avversari e le loro organizzazioni.
3. **Avvisa in privato i tuoi amici, la tua famiglia e le reti politiche sensibili.** Affida ad alcuni amici fidati le tue informazioni personali affinché ti aiutino a segnalare social e blog che di doxxano, identificandoli come persecutori. Fallo ripetutamente. Alcune piattaforme non dispongono di politiche che ti proteggano, anche se questi post includono informazioni personali accurate, anche se ti mettono in pericolo. A volte, i doxxer utilizzeranno le tue foto e le tue informazioni per creare account fasulli. Di solito, è più facile segnalarli come falsi; prova a farlo rapidamente per evitare che ottengano più informazioni dalle tue reti fingendo di essere te. Tu, la tua famiglia e il tuo datore di lavoro potreste iniziare a ricevere telefonate minacciose o persecutorie. Fai saper loro cosa sta succedendo il più rapidamente possibile e istruiscili a non intergire con i persecutori.
4. **Interrompi il flusso d'informazioni.** Se stai leggendo questa sezione e non hai messo in pratica i consigli della sezione dedicata alla prevenzione, inizia da lì. Scarica un gestore di password come LastPass e cambia immediatamente tutte le tue password. Puoi anche pagare per un servizio chiamato Delete Me che eliminerà buona parte delle tue tracce online dai siti snoop che raccolgono e visualizzano informazioni personali. Questo servizio si prenderà cura delle informazioni accumulate dai data broker ma non di qualsiasi social media, account Web, articoli di notizie o precedenti penali che potresti avere, questi dovrai gestirli da solo. È importante bilanciare l'emorragia d'informazioni, e allo stesso tempo non avvisare i persecutori che il dox è stato efficace o ben mirato. Prova a rinforzare i tuoi account sui social rendendo private le liste di amici e le informazioni per proteggere le tue reti finché non sei sicuro che non offrono informazioni personali vulnerabili a coloro che sono disposti a scavare

per ottenerle. Il modo in cui reagisci pubblicamente è una situazione molto delicata e dovrebbe essere gestita con attenzione nel corso di tutto il processo.

5. **Stabilisci un piano d'emergenza.** Recluta amici e familiari che ti sostengano. Fai saper loro cosa sta succedendo; il doxxing può essere traumatico e devi dare la priorità alla tua salute psicofisica in modo da poter elaborare questi attacchi. Queste conversazioni possono essere difficili—soprattutto se i tuoi interlocutori non comprendono le sfumature di questo momento politico, se è la prima volta che sentono parlare di un certo tipo di hate group o se le vostre relazioni sono tese a causa di differenze politiche o personali. Se non te la senti di farlo, potresti chiedere a un amico che comprende bene la situazione di sostenere al posto tuo le conversazioni più difficili.

Se il tuo indirizzo di casa è incluso nel doxx, trova un posto nuovo in cui soggiornare se puoi. Se non puoi uscire di casa, invita gli amici o un gruppo di sicurezza locale a stare con te. Crea una «borsa da viaggio» con tutto ciò di cui hai bisogno se devi fare le valigie e andare via con poco preavviso.

Valuta le minacce

Se ritieni di non essere troppo in pericolo, soprattutto se il tuo doxx è composto da informazioni liberamente consultabili o ti viene semplicemente inviato direttamente nel tentativo di innervosirti, potresti sentirti bene liquidandolo come una tattica intimidatoria da quattro soldi, bloccare e segnalare il persecutore e andare avanti. Potrebbe soltanto trattarsi di qualcuno che cerca di farti arrabbiare. Tuttavia, se il tuo doxx include dati personali sensibili—nello specifico, dettagli non facilmente ottenibili con un semplice lavoro investigativo—o appare in un forum pubblico in cui le persone distribuiscono informazioni nella speranza che altri agiscano su di esso, potresti prendere ulteriori precauzioni. Questo vale soprattutto se fai già parte di un gruppo o di una categoria demografica già presi di mira.

Quando scopri di essere stato doxxato, è importante stabilire quali informazioni potrebbero tradursi in minacce reali. Spesso, il doxxing è il precursore di persecuzioni offline più intrusive o è collegato a minacce

di agire in base alle informazioni. Potrebbe trattarsi di qualsiasi cosa, da telefonate intimidatorie alla famiglia o sul posto di lavoro a minacce di morte mirate o un'incursione della SWAT.

A volte è difficile determinare cosa renda «reale» una minaccia. La tattica più comune dei doxxer mediocri è di inviare messaggi inquietanti o intimidatori ovunque pensino di poterti raggiungere: social, e-mail, familiari e simili. Penseranno spesso di avere più informazioni di quante ne abbiano in realtà; è normale che dicano di aver fornito queste informazioni alle forze dell'ordine locali. Il loro obiettivo è intimidirti per non farti agire; spesso, le informazioni che postano pubblicamente è tutto ciò che hanno.

Il tuo datore di lavoro potrebbe ricevere chiamate che chiedono di licenziarti. Finora, è raro che gli obiettivi di doxxing siano stati attaccati fisicamente, ma * è successo * , ed è possibile che coloro che ti doxxano tentino di mettere le tue informazioni nelle mani di persone che non agiscono in modo razionale o etico. È importante essere cauti ma non farti prendere dal panico o dall'ansia.

Chiediti:

- Le informazioni sono accurate? Hanno il tuo indirizzo, quello del tuo luogo di lavoro, quello della tua famiglia? Sanno quali sono i posti in cui bazzichi? Di chi sei amico?
- Rischi di perdere il lavoro se scoprono una qualsiasi di queste informazioni su di te?
- Sai dove vivono i persecutori? Sono vicini alla tua comunità fisica o sono solo troll online su un forum decentralizzato? Hai motivo di credere che le forze dell'ordine saranno interessate a queste informazioni? Queste vengono condivise da fonti giornalistiche locali di destra che danno la tua faccia in pasto a una marea di estranei ostili che ora sanno delle cose su di te?
- Hanno tue foto imbarazzanti o private?
- Ci sono informazioni che ti legano ad attività criminali che potrebbero farti arrestare?

Soluzioni

Ecco alcune cose che puoi fare in risposta ai pericoli che possono derivare dall'essere doxxato:

- Elabora un piano di autodifesa, iscriviti a corsi di autodifesa, contatta un gruppo di difesa della comunità locale.
- Informa le persone e i gruppi nominati nella doxx: posto di lavoro, compagni, coinquilini, famiglia.
- Parla delle tue paure con le persone di cui ti fidi.
- Contatta le persone che hanno già affrontato questo problema per ricevere dei consigli.
- Organizzati in modo da poter avere un avvocato se temi che le informazioni su di te possano interessare gli attori statali.
- Connettiti con un gruppo antifascista locale: potrebbe essere in grado di aiutare a identificare i doxxer, se questi stanno postando da un account falso.

Parlare al lavoro e in famiglia

Intrattenere questa conversazione può essere molto difficile, soprattutto se tu e la tua famiglia avete rapporti tesi. Cerca di avere un amico dotato di sangue freddo che possa aiutarti a mediare o che possa sostenerti in seguito, se necessario.

Pensa a quanto spesso sei disposto a essere vulnerabile con la tua famiglia e a quante opportunità avrai in futuro per proseguire la conversazione. Se è necessario parlare con i membri della famiglia ma pensi di avere solo una possibilità, puoi esercitarti con un amico e prepararti per le loro reazioni. Se hai una relazione continua, colloquiale e di fiducia, puoi spiegare loro la situazione attraverso una serie di conversazioni più brevi, invece che con un incontro lungo. Valuta quanto tempo e quanta attenzione avrai.

Inquadrare questa situazione nei termini di «avere uno stalker» mi ha sempre aiutato con le persone con cui non voglio avere una conversazione politica—questo può essere sufficiente per spiegare la gravità della situazione e perché hai bisogno di privacy. Ma può valere la pena essere onesti su quel che sta succedendo. Questo può aiutare a costruire relazioni più solide e demistificare questo fenomeno comune, incoraggiando allo stesso

tempo altri che potrebbero non aver considerato che potrebbe accadere a loro o a qualcuno che conoscono a prendere sul serio la privacy online. La maggior parte delle persone risponderà con paura e comprensione, anche se a volte suggeriranno, o addirittura insisteranno, che tu ti rivolga la Polizia.

Non esiste un approccio valido per tutti. Nel mio caso, ho dovuto costringere mia madre conservatrice a promettere che non avrebbe coinvolto la Polizia. Ci sono riuscito facendo appello al mio diritto alla sicurezza personale e alla mia autonomia come vittima della situazione, chiedendole di rispettare i miei desideri e ricordandole che la Polizia può fare molto poco per rispondere a persecuzioni mirate come questa—e che, essendo stato accusato di attività criminale, rivolgersi a loro avrebbe significato farmi sottoporre a esami minuziosi da parte loro. Tali conversazioni possono essere molto difficili ma sono spesso necessarie. Ricorda ai tuoi amici e familiari di non reagire o di non rispondere a telefonate, e-mail o richieste sui social.

Qui[10] puoi leggere una guida su come discuterne con il tuo datore di lavoro.

Cose da ricordare quando parli con amici e familiari:

- L'obiettivo dei persecutori è mettere a dura prova le tue relazioni e rovinarti la vita. Non far sì che ci riescano. Di' alla tua famiglia che il modo migliore per sostenerti è rifiutarsi di cedere alle loro tattiche.
- Non pugnalare alle spalle anarchici e antifascisti e non affermare di essere preso di mira senza motivo. Questo non ti servirà se emergeranno i motivi—e delegittimerà e metterà ulteriormente in pericolo chi non può prendere le distanze dalla politica anarchica.
- Non lasciare che nessuno ti biasimi per ciò che sta accadendo, sia che si tratti della politica di o per la tua percepita irresponsabilità per esserti messo «in questa situazione». Combattere per un mondo migliore comporta sfide. Se non altro, è merito tuo se hai provocato questa risposta con i tuoi sforzi.

[10]https://crashoverridenetwork.com/employers.pdf

- Suggerisci modi concreti per aiutarli a capire la situazione e proteggersi. Invia loro quest'articolo o un elenco di risorse; offriti di aiutarli a bloccare i loro social se non sono esperti di tecnologia.
- Parla di ciò per cui possono prepararsi: telefonate persecutorie, e-mail, forse i vicini riceveranno messaggi su di te. Preparali per lo scenario peggiore ma sottolinea che è improbabile.
- Sii chiaro su ciò di cui hai bisogno da loro.

Vivi la tua vita, andando avanti

Fai un respiro profondo. Non darti colpe. Da un punto di vista emotivo, questo può essere profondamente inquietante e dirompente, aggiungendo uno strato di stress acuto alla tua vita. Potrebbero esserci persone là fuori che sanno che aspetto hai e non avrai idea di chi siano. A volte le informazioni di chi ti doxxa diventano una parte permanente di Internet se il tuo nome viene cercato su Google; questo può influenzare le tue prospettive lavorative. A volte non ne consegue nulla ma c'è sempre la possibilità che qualcuno provi a riprendere da dove si era fermato l'ultimo doxxer.

Finché non sei sicuro che il tuo tempo sotto i riflettori è finito, potresti dover modificare alcuni aspetti della tua vita. Chiediti: «Che tipo di vita voglio vivere? Come posso gestire la mia ansia? Ci sono modi in cui posso accettare di essere una figura più pubblica? Come posso sentirmi sicuro nell'assumere dei rischi e nell'essere di nuovo attivo?» Adottare misure di sicurezza più estreme potrebbe essere importante soprattutto con l'intensificarsi delle tensioni politiche.

Ecco alcune misure che potresti scegliere di utilizzare:

- Non lasciare che nessuno ti fotografi a meno che non ti fidi di loro per gestire le immagini nel modo in cui ne hai bisogno. Questo può dar vita a conversazioni imbarazzanti, soprattutto nel caso di eventi familiari o di situazioni professionali. Fai attenzione a chi appare nelle foto con te; mettili al corrente che apparire in una foto con te potrebbe attirare attenzioni indesiderate. Può essere utile provare le conversazioni che potresti dover avere.
- Installa delle trail camera a casa tua.

- Conserva i registri di tutte le persecuzioni di cui sei vittima.
- Se cambi casa, non aggiornare il tuo indirizzo. Non registrarti per votare, poiché questo rende il tuo indirizzo di dominio pubblico. Prova a conservare la tua vecchia patente o documento d'identità e fatti mandare la posta presso una casella postale. Pensa a quando utilizzare un indirizzo reale e quando usarne uno falso o ometterlo del tutto quando ti registri online o di persona.
- Usa pseudonimi online e di persona, se necessario. Non usare sempre lo stesso.
- Quando prendi parte a un'azione, soprattutto se non copri il viso, sii consapevole di quali gruppi, luoghi o individui potrebbero essere coinvolti essendo visti o fotografati vicino a te.
- Investi del tempo in lezioni di autodifesa. Questo può includere far pratica con le armi ma dovrebbe includere l'addestramento difensivo e atto a disarmare.
- Rivolgiti a un terapista per affrontare qualsiasi trauma subìto.
- Aiuta i tuoi amici e familiari a capire l'importanza della sicurezza online.
- Sostieni conversazioni oneste con persone al di fuori delle tue cerchie di affinità politica. Potresti essere sorpreso dalla quantità di empatia che esprimono.

Non importa quanto le persone che ti prendono di mira provino a farti sentire isolato, non sei solo. In quanto comunità, dobbiamo proteggerci l'un l'altro e dobbiamo proteggere le nostre reti online da persecuzioni, incarcerazioni, violenza politica e intimidazioni. Insieme, **possiamo farlo**.

Questa guida dettagliata spiega come proteggersi dagli stalker online, perché è importante e cosa fare se si è presi di mira dal «doxxing», ovvero la pubblicazione delle proprie informazioni riservate.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.