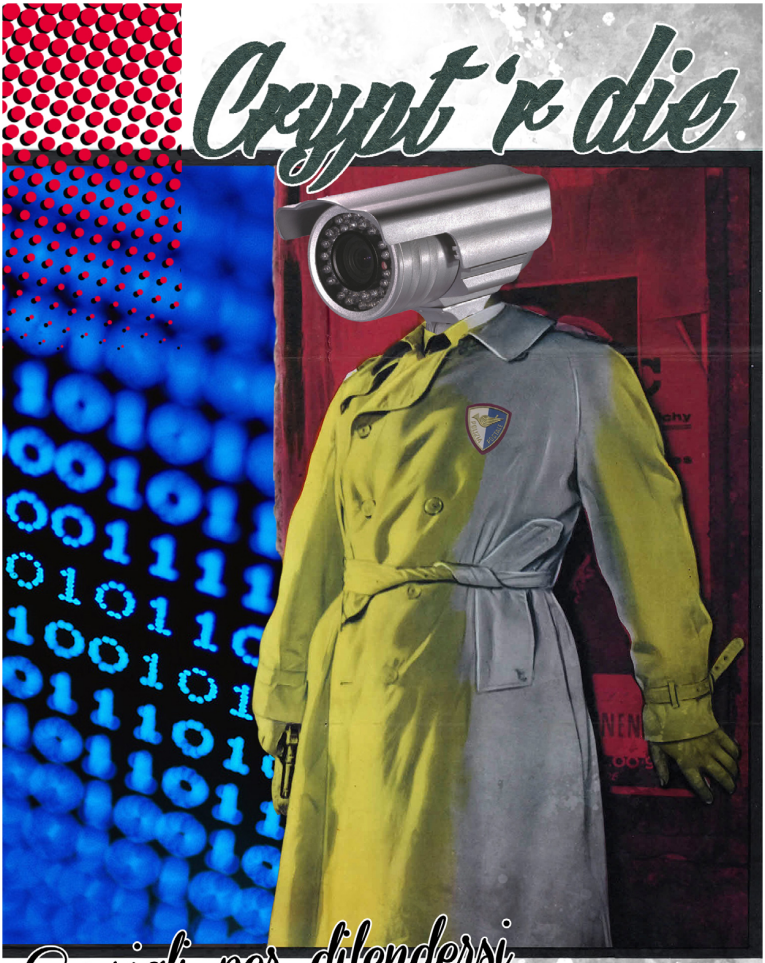
Crypt 'r die



Consigli per difendersi dalla repressione digitale

Il collettivo AvANa (Avvisi Ai Naviganti) fin dalle origini ha dato sempre centralità al tema della repressione a mezzo digitale.

Quando ci è passato tra le mani l'opuscolo "Prima, durante e dopo un corteo", scritto dalla Rete Evasioni, abbiamo letto il paragrafetto dedicato ai computer e non abbiamo saputo resistere. **Crypt'r Die** è un vademecum per tutte e tutti coloro che vogliono iniziare a riprendersi la propria libertà e che sentono il bisogno di difendersi da ogni tipo di controllo e sorveglianza digitale.

Finito di stampare nel giugno 2014.

https://we.riseup.net/avana/opuscolo

INDICE

Repressione e tecnologia: una panoramica

Che la repressione usi le tecnologie non è una novità. Quello che cerchiamo di fare in questo capitolo, dunque, è una panoramica sul problema, cercando di quantificarlo, di capirne i rischi e i margini di azione.

Chi ha qualcosa da nascondere?

Tutti/e.

Sul tuo computer transitano un mare di informazioni delicate: i siti che visiti, le persone con cui parli, i messaggi che ti scambi sono monitorati in modo sistematico, per meglio classificarti. Discorso analogo

vale per smartphone e tablet. Con un po' di analisi è possibile sapere chi sei, dove vivi, chi frequenti, la tua routine, il tuo carattere. Questi dati possono rivelare tanto i tuoi gusti musicali quanto le tue tendenze politiche: la profilazione commerciale va a braccetto con una schedatura di massa.

Non si tratta però solamente di proteggere la propria identità, o fatti specifici legati a reati: monitorando la rete, la polizia cerca soprattutto di capire quali sono i soggetti più attivi all' interno di un gruppo, al fine di rendere più facile un' attività di contrasto.

I miei dati sono al sicuro?

La sicurezza informatica è una materia complessa, proviamo quindi a districarla.

Il tuo computer *contiene* dei dati. Chi controlla il tuo computer ha il pieno accesso ai tuoi dati. Non è così improbabile che qualcuno lo faccia: accessi fisici (computer lasciati incustoditi) o software (attraverso internet) avvengono quotidianamente.

Il tuo computer *comunica*. Ogni volta che chatti, videochiami, scrivi email, ti connetti a dei social network, invii foto o ascolti musica, il tuo computer scambia messaggi con altri computer e server. Qualcuno potrebbe *ascoltare* queste comunicazioni.

Molti dei *servizi* che usi su internet controllano i tuoi dati. Le aziende (google, facebook, microsoft, yahoo...) tengono traccia di ogni possibile informazione su di te, e puoi stare certo che le inoltreranno alle autorità non appena richiesto. Stai quindi delegando i tuoi dati alla loro gestione. Ti fidi di loro?

Per finire, ricorda che la gestione della tua sicurezza è principalmente un approccio mentale. Spesso è necessario prestare particolare attenzione: ad esempio nell'usare il computer di un tuo amico o quelli di un *internet point* potresti lasciare lì le tue password, permettendo ai visitatori successivi di vedere i tuoi dati.

Con i piedi per terra

È naturale è chiedersi quanto siano realistici questi problemi e *chi* sia materialmente in grado di compiere degli attacchi informatici per impadronirsi dei tuoi dati. Alcuni attacchi sono accessibili a molti, altri richiedono risorse e capacità meno comuni.

Ad esempio, un collega invadente potrebbe leggere le tue email mentre ti allontani dal computer per una pausa. La polizia, invece, preferisce sequestrarti il computer per fare analisi approfondite: sta a te fare in modo che queste analisi non portino a nulla!

Situazioni e soluzioni diverse quindi, a seconda del tipo di attacco del quale si diventa bersaglio.

Malware

Tutti sappiamo cos'è un virus. Un Malware è un programma simile a un virus che ha lo scopo di ottenere il controllo del tuo computer, trasformandolo in una sorta di microspia altamente tecnologica. Questa tecnica è sempre più usata dalle polizie di tutto il

mondo, ed è decisamente la più potente. C'è qualche evidenza di uso anche da parte della polizia italiana.

Ci si può proteggere innanzitutto smettendo di utilizzare sistemi operativi proprietari (Microsoft Windows e Mac OSX) dal momento che sono decisamente più controllabili rispetto ad esempio a GNU/Linux (sebbene anche un utilizzo sconsiderato di Linux possa comportare dei rischi).

Problemi simili si riscontrano anche nelle applicazioni, un esempio significativo è Skype: è infatti noto che questo programma non solo è monitorato dalle polizie, ma viene addirittura utilizzato per controllare tutte le attività del computer. Possiamo quindi dire che Skype è un malware.

Grazie alle pubblicazioni di Wikileaks nella pagina degli Spy Files [1] è possibile avere un quadro sulla diffusione dell' industria di sorveglianza mondiale. In questa pagina [2] invece, abbiamo iniziato a raccogliere le inchieste in cui è stato utilizzato il malware come strumento di intercettazione.

[1] http://wikileaks.org/The-Spyfiles-The-Map.html
[2] https://we.riseup.net/avana/malware-di-stato

Sequestro

Con un mandato, la polizia può sequestrare materiale informatico a scopo di indagine. Nel dubbio, la polizia sequestra tutto quello che può (computer, penne USB, fotocamere, registratori. . .).

Dopo il sequestro, la polizia prende possesso di tutto ciò che trova su computer e hard disk. Se i dati del computer non sono cifrati, la polizia può facilmente accedere alle password che hai salvato sul tuo computer, ai tuoi documenti, alla cronologia (del browser, delle chat etc.) e, se usi un client di posta, alle tue e-mail.

La migliore soluzione contro questo attacco è criptare il proprio disco.

Richiesta di dati al fornitore di servizi

La maggior parte dei servizi che utilizzi sono online: email, social network e altri. La polizia può chiedere alle aziende che gestiscono tali servizi tutto ciò che è possibile sapere su una certa email o su uno specifico

account: solitamente vengono richiesti i contenuti delle comunicazioni e gli indirizzi IP da cui l'utente si è collegato. Anche senza mandato.

Cancellare i dati sui nostri account online non ci da garanzia alcuna. Ad esempio, Facebook e forse anche altre aziende mantengono nei propri server una copia dei dati che l'utente ha cancellato dal suo account, per un certo periodo di tempo. Altre aziende favoriscono la persistenza dei dati sui loro server. Ad esempio, GMail scoraggia la cancellazione delle email mettendo a disposizione di tutti uno spazio di memorizzazione molto grande e propone la archiviazione delle vecchie comunicazioni invece che la cancellazione delle stesse.

Intercettazioni

Le comunicazioni che effettui tramite Internet attraversano le infrastrutture del tuo provider (fastweb, alice, tiscali, . . .). Alcune di queste comunicazione sono cifrate, ed è quindi molto complicato leggerne il contenuto, ma molte altre invece non lo sono:

vengono definite “in chiaro”. In sostanza, una buona parte delle tue comunicazioni è perfettamente leggibile dall’ amministratore della tua rete così come dall’ azienda che ti fornisce connettività.

Il tuo fornitore di ADSL o di telefonia mobile potrebbe inoltre collaborare con la polizia permettendole di controllare ciò che fai. Questa tecnica di controllo è tecnologicamente meno potente dei malware, visto che l’uso della crittografia la può inibire.

Dal punto di vista legale, questa procedura è del tutto equivalente ad una “intercettazione telefonica”.

Legal

La perquisizione informatica

Come funziona

Se ti trovi in un luogo pubblico è possibile per la polizia chiedere di controllare il tuo computer (o smartphone) senza necessità di mandato o giustificazione.

Come comportarsi

Per quanto riguarda il portatile, una semplice soluzione è abbassare lo schermo: la maggior parte dei sistemi chiede una password per sbloccare lo schermo. A quel punto, se la password non è troppo facile (ad esempio uguale al nome utente) difficilmente sarà possibile accedere al sistema con una semplice perquisizione.

Ricordati che non sei tenuto a dire la password, oltre al fatto che è sempre ammessa l' eventualità di non ricordarla.

Per gli smartphone sono disponibili metodi simili per mettere un blocco allo schermo, spesso in modo molto semplice.

Il sequestro

Il caso del sequestro è differente: si tratta tipicamente di un evento organizzato in cui la polizia entra in un domicilio per sequestrare oggetti utili alle indagini. La perquisizione di domicilio necessita, nor-

malmente, di mandato. È però possibile subire una perquisizione domiciliare senza mandato se finalizzata alla ricerca di armi o droga; in questo caso la polizia non può sequestrare nulla che non sia armi o droga.

Ecco alcune raccomandazioni:

- Spegnere i computer o “bloccarli” (ad esempio attivando lo screensaver del portatile): questo, più che per il sequestro in sé, serve ad evitare che sia condotta *anche* una perquisizione.
- Verificare che siano posti i sigilli su tutto il materiale sequestrato, compresi computer, hard disk . . . ; se questo non avviene, chiedere che sia messo a verbale.
- Richiedere la presenza di un perito di parte durante il sequestro. Chiunque può esserlo (ovviamente una persona con competenze informatiche risulta maggiormente credibile).
- Richiedere la presenza di un avvocato.
- Se ti vengono richieste le password non sei obbligato a darle. Non ricordare è meglio che

negare e porsi in un atteggiamento ostile. Considera però che se il computer non è cifrato, tutte le password ivi memorizzate saranno violate con estrema semplicità, ad esempio quella di avvio di Windows oppure la password del tuo servizio on line preferito.

- Se il tuo computer è già acceso e viene usato da polizia o periti durante il sequestro, chiedi che sia messo a verbale. A maggior ragione se era spento e viene acceso.

Dopo il dissequestro (ovvero alla riconsegna del materiale) **non** accendere per nessun motivo i dispositivi, per non precludere la possibilità di una eventuale controperizia. Avvisa invece un esperto informatico di tua fiducia. Continua online [3].

[3] https://we.riseup.net/avana/opuscolo-legal

Ricette per la tua sicurezza

Un computer sicuro

Utilizzare programmi sicuri su un computer non sicuro è poco utile; allo stesso modo, nessuna tecnica crittografica ci proteggerà da una password banale. Una porta blindata è inutile, se lasci la chiave sotto lo zerbino. Quelle che seguono sono ricette sempre valide, qualsiasi cosa tu voglia fare con il computer.

Abbandonare Windows e Mac

Difficoltà di configurazione: media (se vuoi installare GNU/Linux a fianco di un altro sistema operativo), facile (se vuoi installare solo GNU/Linux), facilissima (se usi freepto)
Difficoltà quotidiana: media
Utile contro: malware

Un malware è un programma che esegue operazioni arbitrarie su un computer senza che noi riusciamo ad accorgercene. Anche se ancora non molto diffuso

è il più pericoloso tra gli attacchi al quale possiamo essere soggetti perché permette l'accesso completo al nostro computer e, di conseguenza, anche a tutti i nostri dati. Ad esempio, la polizia li utilizza per controllare gli indagati attraverso la webcam e il microfono del loro computer.

L'utilizzo di malware come strumento di intercettazione si sta diffondendo e il target più vulnerabile a questo tipo di attacco è il sistema operativo Microsoft Windows. Anche Mac OS X non è esente da attacchi. Non sono invece noti attacchi seri a GNU/Linux. Il rimedio migliore per proteggersi da questo genere di attacco è abbandonare Windows a favore di un sistema operativo open source come GNU/Linux ed acquisire un po' di destrezza nel suo utilizzo.

Ad esempio puoi usare freepto. Vedi l'ultimo capitolo per maggiori informazioni.

Cifrare i propri dati

Difficoltà di preparazione: facilissima con Freepto, facile se hai un Mac, facile se installi da zero GNU/Linux, medio/difficile in tutti gli altri casi
Difficoltà quotidiana: minima
Utile contro: sequestro

Per proteggere i dati dal sequestro, la soluzione più semplice ed efficace è la cifratura del disco. Nella pratica, questo richiede l'inserimento di una pas-

sword all' avvio del computer. Se la password è sufficientemente complessa e viene mantenuta segreta, il contenuto del disco sarà indecifrabile. La cifratura del disco di sistema non protegge dati messi su penne usb o dischi esterni.

Un ulteriore motivo per scegliere di cifrare il disco è la possibilità di scaricare le email con Thunderbird, cancellandole dai server di posta e custodirle al sicuro sul tuo disco cifrato.

Questo non ti protegge però dai malware: per evitarli, il consiglio migliore che possiamo darti è Abbandona Windows e Mac (vedi pagina 11). Continua online [4].

Password

Difficoltà quotidiana: facile
Utile contro: accessi non autorizzati

Una password "sicura" aiuta a prevenire accessi indesiderati al tuo account. Spesso, per pigrizia, si imposta una stessa password per accedere a più

[4] https://we.riseup.net/avana/opuscolo-crypto

servizi in rete. Inoltre, password semplici possono essere indovinate da programmi appositi.

È bene condividere alcune considerazioni per la gestione di una password:

- Non dovresti usare password importanti in contesti non sicuri (internet point, computer di persone non fidate o di persone di cui ti fidi “personalmente” ma non tecnicamente); comunque, a volte questo succederà. In questo caso, cambia la password (da un computer fidato) appena puoi.
- Non usare password facili: il tuo nome, la tua data di nascita o altri dati noti. Non usare parole semplici, usa combinazioni di lettere MAIUSCOLE e minuscole, combina numeri e simboli. Lunghezza minima consigliata: 8 caratteri.
- Non condividere le password se non è proprio assolutamente necessario.
- Diversifica il più possibile le password e comunque utilizza sempre password diverse per contesti diversi (ad esempio utilizza password di-

verse per la mail di lavoro, per la mail su server commerciali e per la mail su server autogestiti come Autistici/Inventati o Riseup).

- Se il tuo computer non è cifrato, le password che memorizzi sul tuo browser saranno registrate in chiaro; valuta quindi di non salvare affatto quelle particolarmente sensibili (o meglio, cifrati il disco!).

Cancellazione sicura dei file

Difficoltà di configurazione: media; su freepto: già configurato
Difficoltà quotidiana: facilissimo
Utile contro: sequestro del computer

Quando cancelli i dati sul tuo PC rimangono comunque delle tracce sul disco ed è possibile, per un tecnico forense, recuperarli completamente o in parte attraverso l'uso di opportuni software. Alcuni programmi però permettono la cancellazione sicura dei tuoi file, così che sia impossibile recuperarli

successivamente. Continua online [5].

Comunicare

Le comunicazioni personali e quotidiane sono le operazioni più sensibili che fai in rete e, probabilmente, sono già state osservate dal tuo provider adsl o di posta elettronica. Quindi, o ti trovi un provider meno impiccione oppure fai in modo che il provider non possa leggere le tue comunicazioni. Ti consigliamo di seguire entrambi questi consigli.

[5] https://we.riseup.net/avana/opuscolo-wipe

Usare servizi autogestiti

Difficoltà di configurazione: facile
Difficoltà quotidiana: facilissima
Utile contro: identificazione, richiesta dati al fornitore di servizi, profilazione

I servizi autogestiti sono delle piccole isole nella rete, spazi aperti dove individualità e collettivi forniscono strumenti e servizi di comunicazione liberi. Questi servizi sono gratuiti per tutti/e, ma hanno un costo per chi li rende disponibili: sostienili con benefit e donazioni!

I servizi autogestiti (riseup.net, autistici.org, indivia.net, tracciabi.li) prendono contromisure per evitare di fornire informazioni su di te alle autorità.

Inoltre questi servizi mettono al centro delle priorità l'utente invece dei profitti. Questo li porta a fare scelte molto migliori nei tuoi confronti. Ad esempio, Gmail ti "sconsiglia" di cancellare le email, altri servizi commerciali ti incentivano ad abbinare un numero di cellulare al tuo account. Nessun server autogestito di chiederà mai di fare cose simili.

Utilizzare servizi autogestiti è veramente semplice: per richiedere una email su autistici.org vai su [6] e compila il modulo. Dopo qualche giorno la tua email verrà attivata. Continua online [7].

Chat sicura

Difficoltà di installazione: media, già installato su freepto
Difficoltà di configurazione di OTR: media
Difficoltà quotidiana: facile Utile contro: intercettazioni

Gli strumenti più diffusi per l'Instant Messaging (Skype, GTalk, Facebook Chat, Yahoo! Messenger, etc) "proteggono" le tue comunicazione attraverso l'uso della cifratura SSL (o TLS). Questo rende più difficile ad un coinquilino o ad un collega troppo curioso di leggere facilmente le tue conversazioni. In questi casi, la tua privacy è totalmente gestita delle aziende a cui ti affidi per comunicare; non c'è alcun buon motivo per credere che di fronte alla richie-

[6] https://services.autistici.org/
[7] https://we.riseup.net/avana/opuscolo-servizi

sta della magistratura queste aziende intraprendano delle azioni per la tutela della tua privacy.

Esistono però delle soluzioni:

I server autogestiti A/I [8] e Riseup [9] offrono ai loro utenti Jabber (XMPP), uno strumento molto diffuso di Instant Messagging. Peraltro, il servizio viene automaticamente attivato per chiunque abbia una mail con uno di questi server autogestiti. Inoltre, per aumentare la tua privacy puoi utilizzare OTR (Off-the-Record), una tecnologia che permette la cifratura di tutte le tue conversazioni in maniera semplice. Quando utilizi OTR nemmeno A/I o Riseup sono in grado di leggere le tue conversazioni e puoi essere sicuro che nessuno ti sta intercettando.
Continua online [10].

Usa GPG con Thunderbird + Enigmail

[8] https://www.autistici.org
[9] https://www.riseup.net
[10] https://we.riseup.net/avana/opuscolo-im

Difficoltà di configurazione: media
Difficoltà quotidiana: media; se hai un gruppo con cui parli prevalentemente, facile
Utile contro: Intercettazione

È ormai risaputo che utilizzare servizi commerciali toglie ogni riservatezza alle tue comunicazioni. Ad esempio, nulla impedisce a Google di leggere tutte le tue conversazioni, consegnarle alle forze dell' ordine o analizzarle per proporti della pubblicità mirata. Anzi.

Anche se usi servizi più fidati, come Autistici/Inventati, Riseup, Indivia o Ortiche, buona norma di sicurezza consiste nell'inviare messaggi di posta elettronica che non sono leggibili a chi gestisce la tua casella email.

Per proteggere la riservatezza delle tue comunicazioni puoi utilizzare GnuPG, un software crittografico che si integra molto bene con Thunderbird [11].

[11] https://we.riseup.net/avana/opuscolo-gpg

Audio/Video chat

Per fare audiochiamate (o videochiamate) ci sono varie soluzioni. Purtroppo nessuna di esse è perfetta.

Audio/video chat a due

Difficoltà di installazione: media, già installato su Freepto.
Difficoltà di utilizzo: facile
Utile contro: intercettazione, skype!

Abbiamo già parlato di Jabber e di Pidgin. Questi supportano chat audio/video tra due persone senza problemi: il grado di riservatezza non è molto elevato, ma è sicuramente molto meglio che usare skype! Il vantaggio principale è che se usi Pidgin per la chat con OTR, non serve nessuna configurazione aggiuntiva per usarlo anche per le videochiamate [12].

Audio chat di gruppo

[12] https://we.riseup.net/avana/opuscolo-jabber-av

Difficoltà di installazione: media
Difficoltà di utilizzo: facilissima
Utile contro: intercettazione, skype!

Mumble è un software molto comodo per gestire chat di gruppo in modo semplice e pratico: l'unica leggera difficoltà di installazione è la configurazione del microfono. Rispetto ad altri software commerciali (ad esempio skype) si ha anche una migliore qualità del suono e della conversazione, soprattutto in gruppi molto grandi. Ovviamente nulla impedisce di utilizzarlo anche per chiamate tra due sole persone. La riservatezza delle conversazioni non è particolarmente robusta: paragonabile ad uno scambio di email senza l'utilizzo di crittografia [13].

Audio/video chat cifrata

Difficoltà di installazione: medio-difficile
Difficoltà di utilizzo: facile
Utile contro: intercettazione, skype!

[13] https://we.riseup.net/avana/opuscolo-mumble

Jitsi permette di fare chiamate audio/video usando la cifratura ZRTP, che può essere considerata "analoga" ad OTR. La cifratura è quindi completa, il meccanismo di verifica semplicissimo. Jitsi è un buon software ed è semplice da usare: il principale difetto è che la configurazione di default lascia molte tracce sul computer, e vanno quindi cambiate alcune opzioni per poterlo usare in maniera sicura [14].

Navigare in rete

Tutta la tua attività in rete può essere tracciata facilmente. La maggior parte dei siti web tengono traccia degli indirizzi IP dei loro visitatori. Questi dati possono essere utilizzati a posteriori per identificare l'autore di un contenuto pubblicato su Internet. Per questo motivo non è sufficiente utilizzare uno pseudonimo per proteggere la nostra reale identità. Esistono software che ci danno la possibilità di rimanere anonimi durante la navigazione con il browser su internet:

[14] https://we.riseup.net/avana/opuscolo-jitsi

Usa Firefox + HTTPS Everywhere

Difficoltà di configurazione: facile, su freepto: già configurato
Difficoltà quotidiana: nessuna
Utile contro: intercettazione

Le comunicazioni su internet possono essere in chiaro (ovvero leggibile da chiunque) o cifrate (ovvero leggibile solo dal mittente e dal destinatario). Molti servizi online offrono la possibilità di comunicare in chiaro e in maniera cifrata ma il nostro browser (Firefox) non sceglie automaticamente la modalità cifrata. HTTPS everywhere è un'estensione disponibile per Firefox e Chrome/Chromium che risolve questo problema.

Basta un click per installarla e si guadagna *molto* in termini di sicurezza: le intercettazioni delle comunicazioni cifrate sono infatti molto difficili, e possono essere condotte solo da attaccanti molto motivati [15].

TorBrowser

[15] https://we.riseup.net/avana/opuscolo-https

Difficoltà di configurazione: facile, su freepto: facilissima
Difficoltà quotidiana: facile, ma la navigazione è molto rallentata
Utile contro: identificazioni; intercettazione delle comunicazioni

È una versione modificata di Firefox già configurata per utilizzare la rete Tor. TorProject.org è una rete di server, sviluppata e gestita dal lavoro di associazioni in difesa dei diritti digitali e da individualità di tutto il mondo. Tor fa rimbalzare il tuo traffico internet da una nazione all' altra prima di giungere a destinazione. Questo processo rende impossibile, ad ora, l' identificazione di chi lo usa attraverso l'indirizzo IP [16].

VPN autistici/riseup

Difficoltà di configurazione: media/difficile
Difficoltà quotidiana: facile
Utile contro: identificazione; intercettazione delle comunicazioni

[16] https://we.riseup.net/avana/opuscolo-torbrowser

Una VPN permette di proteggere il flusso di dati prodotto dalla tua navigazione inserendolo in una sorta di canale virtuale cifrato (tecnicamente chiamato tunnel). Questo ti permette di tutelare piuttosto efficacemente il tuo anonimato e ti protegge dal rischio di intercettazioni sulla tua linea ADSL casalinga.

A differenza del TorBrowser (tendenzialmente più sicuro) che anonimizza il traffico generato dal tuo browser, la VPN cifra ed anonimizza tutto il traffico internet generato del tuo computer (client mail, client instant messaging, client ftp, etc.)

I server autogestiti Autistici/Inventati e Riseup forniscono un servizio VPN per i loro utenti; tuttavia, è importante comprendere che esse **non** forniscono anonimato, ma solo "confidenzialità": sono cioè utili per "superare" in modo sicuro condizioni di rete svantaggiose come ad esempio reti aziendali, hotspot pubblici o anche la propria linea casalinga, se si suppone che essa possa essere controllata [17].

[17] https://we.riseup.net/avana/opuscolo-vpn

Sicurezza del tuo telefono

Il cellulare è lo strumento tecnologico più diffuso in assoluto, per questo vale la pena chiedersi come utilizzarlo nel modo migliore. Il primo problema da affrontare riguarda l'utilizzo della rete GSM; situazione più complessa si registra nell'utilizzo degli smartphone: le loro funzioni avanzate offrono opportunità aggiuntive e introducono nuovi problemi.

Fonia

Tutti i cellulari si appoggiano alla rete GSM. Questo ha già delle implicazioni di sicurezza.

Quando usi il cellulare la tua posizione viene continuamente comunicata al tuo operatore con un'approssimazione di circa 50 metri. Inoltre esistono sistemi di monitoraggio "preventivo", in grado cioè di rilevare i movimenti di un dispositivo in tempo reale interpretando i comportamenti abituali e "anomali" e allertando le autorità nel caso di aggregazioni di soggetti attenzionati.

I tabulati telefonici e gli sms di ciascun cittadino sono archiviati per almeno 2 anni (spesso di più) e sono accessibili in qualsiasi momento dalla polizia. Questi dati, apparentemente innocui, sono in realtà utilissimi anche semplicemente per individuare nuovi soggetti da sorvegliare.

Tutte le telefonate effettuate sono intercettabili dagli operatori e di conseguenza da polizia e magistratura. Tale possibilità nella realtà viene ampiamente sfruttata: benché solo una piccola parte delle intercettazioni sia utilizzabile come prova in sede processuale, le intercettazioni sono particolarmente diffuse a scopo investigativo, anche nei confronti di chi non è indagato. Per concludere, sebbene le telefonate siano molto monitorate, sono leggermente preferibili agli sms.

Smartphone

Non tutti i cellulare sono uguali, alcuni sono più evoluti di altri. Parliamo di smartphone. Questi dispositivi, che sono veri e propri computer leggeri ed

estremamente portatili possono generare traffico e comunicare in rete (wifi/3G) e possono essere “estesi” attraverso l’installazione di nuove applicazioni. Esistono poi altri tipi di cellulare, che chiameremo i featurephone, i quali offrono le stesse possibibilità degli smartphone anche se si presentano meno usabili e meno accattivanti.

Smartphone e featurephone offrono modalità di comunicazione aggiuntive rispetto ai vecchi cellulari quali e-mail, chat, social network.

Queste possibilità si possono tradurre in minacce.

Ad esempio, le applicazioni che installiamo con tanta facilità potrebbero rivelarsi dei malware e trasformare il nostro smarphone in una microspia ultra portatile: questa eventualità si è già tradotta in realtà in molte occasioni. Occorre quindi cautela nello sceglire quali applicazioni installare, evitando l’installazione compulsiva.

Non solo le app possono avere secondi fini: lo stesso “market” è in realtà un sistema capace di installare ciò che vuole di sua iniziativa sul nostro dispositivo.

Questo dà un potere enorme alle aziende che lo controllano, e non può tranquillizzarci.

La localizzazione degli smartphone è ancora più precisa (raggiungendo una precisione di pochi metri) che con il GSM: grazie all' utilizzo di GPS e reti Wi-Fi, qualsiasi applicazione può ottenere informazioni molto dettagliate sui tuoi spostamenti.

Uno smartphone è a tutti gli effetti un computer tascabile, e se utilizzato in maniera opportuna può avere diversi vantaggi rispetto ad un cellulare tradizionale: la possibilità di scattare foto e metterle online rapidamente, ad esempio, è di grande utilità per un attivista; anche la disponibilità di chat cifrate è sicuramente più attraente degli SMS, ma dobbiamo ricordarci che gli smartphone non possono essere considerati uno strumento sicuro al 100%.

In particolare, ci sentiamo di sconsigliare fortemente gli smartphone BlackBerry ed Apple (iPhone e iPad). Anche gli smartphone Android non sono esenti da problemi, ma lasciano la possibilità di un uso abbastanza sicuro ad un utente cosciente. Una guida

completa alla sicurezza del proprio smartphone sarebbe troppo lunga per questo opuscolo: quelle che forniamo qui sono ricette per usare gli smartphone a fini di mediattivismo o per ottenere un livello di sicurezza tale da poter essere violato ma solo con un considerevole investimento di tempo e denaro.

ObscuraCam: anonimizzare le immagini

Difficoltà di installazione: facile
Difficoltà utilizzo: facile
Utile contro: identificazioni

Se scatti delle foto con il tuo smartphone durante un corteo faresti bene ad editarle in modo da rendere i volti delle persone irriconoscibili se pensi di conservarle o se pensi di condividerle su un social network. Nei processi contro gli attivisti i riconoscimenti attraverso le foto rappresentano spesso una prova decisiva. Inoltre ricorda che spesso non è sufficiente coprire solamente il volto, ma è necessario anonimizzare anche: spille, indumenti e tutti gli altri accessori utilizzabili per l' identificazione. Inoltre sia

Facebook che Google utilizzano software capaci di riconoscere automaticamente il volto delle persone fotografate ed associargli un'identità reale. Non sempre puoi prevedere l'esito di un corteo, per questo motivo se pubblichi "in diretta" le tue foto sui social network ricorda sempre che possono mettere in pericolo le persone coinvolte anche se stai fotografando una situazione al momento tranquilla; ad esempio potrebbe succedere di fotografare una persona che si è assentata dal posto di lavoro per essere in piazza, e la diffusione di questa foto potrebbe causargli molti problemi. Inoltre ricorda che durante un corteo il tuo materiale fotografico può essere posto a sequestro se vieni fermato dalle forze dell' ordine, quindi se le tue foto possono mettere in pericolo delle persone evita di farle.

Obscuracam è un'applicazione per Android che rende semplicissimo e semi-automatico l' offuscamento delle facce e ti permette di editare velocemente le foto prima di pubblicarle online [18].

[18] https://we.riseup.net/avana/opuscolo-obscuracam

Xabber: Chat sicura

Difficoltà di installazione: facile
Difficoltà quotidiana: facile, con OTR: media
Utile contro: intercettazioni

Xabber è una app android di messaggistica istantanea che supporta nativamente TOR e OTR, quindi ti permette di essere confidenziale e anonimo/a. Come Pidgin, Xabber utilizza il protocollo Jabber (vedi capitolo) e quindi ti permette di fare chat a due o di gruppo. Con Xabber puoi comunicare sia con altri Xabber che con Pidgin ma ricordati che su uno smartphone non sei al sicuro quanto su un computer con GNU/Linux [19].

TextSecure

Difficoltà di configurazione: facile
Difficoltà quotidiana: media
Utile contro: intercettazioni, perquisizioni

[19] https://we.riseup.net/avana/opuscolo-xabber

TextSecure, è una app android che ti consente di inviare messaggi in modo riservato sia tramite SMS sia tramite internet. Supporta anche le chat di gruppo.

TextSecure permette di inviare SMS in chiaro anche a chi non ha questa applicazione. Queste comunicazioni non sono cifrate e quindi necessario porre attenzione a come si utilizza questa app.

Rispetto a Xabber, TextSecure ha queste differenze:

- non occorre configurare un account;
- funziona anche senza connessione internet, usando SMS;
- non può comunicare con utenti iPhone e di computer;
- l'interfaccia è un po' confusa ed è facile inviare messaggi non cifrati credendo che lo siano (controlla la presenza del lucchetto prima di inviare!) [20].

Carte telefoniche prepagate

[20] https://we.riseup.net/avana/opuscolo-sms

Difficoltà: facile
Utile contro: intercettazioni

In molte nazioni è posibile acquistare carte SIM prepagate senza fornire un documento di identità durante l'acquisto.

Tutti i telefoni posseggono però un identificativo chiamato IMEI che viene trasmesso durante ogni telefonata. Cambiare la scheda telefonica che usate quotidianamente con una acquistata in maniera anonima potrebbe non garantire il vostro anonimato completo, dal momento che potrebbe essere comunque possibile identificare il vostro telefono. Serve quindi abbinare una scheda anonima con un cellulare non associato alla vostra identità.

Utilizzare computer pubblici

A volte, non è possibile utilizzare il proprio computer. Per controllare la posta o navigare su internet vengono usati computer "pubblici", ad esempio in un'internet point. In queste occasioni è importante

ricordarsi di:

- il *“private browsing”* (anche detto Incognito

Mode in google chrome), una modalità in cui la cronologia e le password non vengono salvate [21].

- *fare logout* dai tuoi account, altrimenti il successivo utilizzatore del computer avrà accesso ai tuoi dati!
- ricorda che un computer pubblico è *inaffidabile* per definizione: meglio non far passare password o dati sensibilii su di esso. Una buona pratica rimane quella di separare gli ambiti, mantenendo account separati per argomenti (ed esposizioni legali) diversi.

Un'altra attenzione da porre è alle *telecamere*: queste vengono usate per leggere ciò che state scrivendo, osservando lo schermo o addirittura le dita che digitano sulla tastiera. Questo pericolo, ovviamente, riguarda anche l'uso di computer proprio in luoghi pubblici (biblioteche, bar, . . .). È molto difficile proteggersi da questo tipo di attacchi, ma alcuni suggerimenti sono:

[21] https://we.riseup.net/avana/opuscolo-private

- coprire una mano con l’altra quando si digitano le password; se si decide di salvare le password sul browser questa azione va fatta una tantum, quindi non è particolarmente noiosa.
- evitare di accedere a contenuti delicati

Freepto

Freepto è un sistema operativo installato su una pennetta usb. Questo significa che puoi portare la pennetta sempre con te ed utilizzare qualsiasi computer proprio come se fosse il tuo portatile. Inoltre i dati che salverai all' interno di questa pennetta saranno automaticamente cifrati (ovvero non potranno essere letti da nessun altro).

Puoi scaricare Freepto e trovare ulteriori informazioni a partire da questa pagina: [22]

Quali sono le caratteristiche principali di Freepto?

Pensata per gli attivisti

Esistono molte distribuzioni GNU/Linux orientate alla sicurezza ed alla privacy, Tails [23] è forse la più famosa di questo genere di distribuzioni. Queste di-

[22] https://www.freepto.mx
[23] https://tails.boum.org/

stribuzioni sono chiamate “live” ovvero offrono un sistema operativo pulito ogni volta che le utilizziamo, perché rimuovono in fase di chiusura tutti i dati prodotti dall’ utente. Inoltre sono pensate per affrontare scenari di repressione veramente molto elevati, dove ad ogni singola azione va prestata attenzione, questo le rende distribuzioni difficilmente utilizzabili nelle attività quotidiane.

L’idea che sta alla base dello sviluppo di Freepto è quella di offrire un sistema operativo semplice che permetta la gestione sicura degli strumenti utilizzati più di frequente dagli attivisti, senza però rinunciare alla comodità di un sistema operativo tradizionale.

Posto che abbandonare l’utilizzo di sistemi operativi proprietari (Windows e Mac OSX) è il primo passo necessario per aumentare la nostra sicurezza, ci sono moltissimi casi in cui abbandonare completamente l’utilizzo di questi sistemi proprietari diventa difficile (magari per necessità lavorative), ed è per questo motivo che diventa importante trovare un modo pratico e veloce per separare l’account utilizzato a lavoro dall’ account utilizzato per fare attivismo.

In questo senso Freepto permette di proteggere attraverso la crittografia i nostri dati e di poterli portare sempre con noi.

AVVISO: Freepto può amentare notevolmente il tuo livello di sicurezza, ma se pensi di trovarti in una situazione che meriti una paranoia aggiuntiva, ti consigliamo di utilizzare TAILS e di approfondire la tua conoscenza degli strumenti che servono a proteggere il tuo anonimato e la tua privacy così da avere ben chiari i limiti e i rischi che derivano dall' uso di queste tecnologie.

Sempre con te

Freepto è un sistema operativo completo dentro una penna usb. La puoi usare da qualsiasi computer ed avrai tutto ciò che ti serve.

Cifrata

I dati contenuti nella penna usb sono cifrati, quindi solo tu puoi leggerli.

Tutto incluso

Freepto contiene molti dei programmi utili: browser, lettore di posta, editor di immagini... e se qualcosa manca, lo si può sempre installare grazie a synaptic, il gestore dei pacchetti presente anche in debian e ubuntu.

Preconfigurata per la sicurezza

Abbiamo cercato di rendere freepto più sicura possibile senza che questo peggiorasse in alcun modo l'esperienza dell' utente:

- i programmi di chat e filezilla sono configurati per l'utilizzo di tor, in modo da avere connessioni anonime e sicure.
- firefox include delle estensioni per cifrare la comunicazione con i server il più possibile
- con firefox si può navigare verso i siti `.onion` (siti interni alla rete tor la cui posizione è nascosta)

Paranoia aggiuntiva opzionale

Abbiamo incluso dentro freepto una serie di tool per chi vuole aumentare ulteriormente il proprio livello di sicurezza:

- cancellazione sicura dei file
- rimozione di metadati contenenti informazioni sensibili su immagini, file audio, pdf e molto altro
- truecrypt, per gestire archivi cifrati
- torbrowser-launcher [24], per avere sempre l'ultima versione di torbrowser e navigare in modo anonimo
- gpg, per scambiarsi mail cifrate
- pidgin-otr, per avere chat sicure in modo molto semplice
- tortp, per forzare l'uso di TOR a tutte le applicazioni che utilizzano la rete
- florence, per avere una tastiera virtuale dove inserire le tue password

[24] https://github.com/micahflee/torbrowser-launcher

- tomb, per la gestione avanzata degli archivi cifrati

Personalizzabile

Lo sviluppo di freepto è basato su Debian Live Build [25], un insieme di tool che permettono di generare delle distribuzioni live personalizzate basate su Debian (GNU/Linux).

Questo significa che puoi contribuire a migliorare freepto e modificarne la configurazione per personalizzarla secondo le tue esigenze. Se sei uno sviluppatore e sei interessato a contribuire a freepto puoi farlo modificando il nostro repository su GitHub [26].

Come si usa?

In questa pagina abbiamo raccolto la documentazione e qualche piccolo tutorial su come configurare

[25] http://live.debian.net
[26] https://github.com/AvANa-BBS/freepto-lb

freepto [27].

È importante che tu legga la documentazione attentamente e se qualcosa non ti è chiaro potrai sempre utilizzare i commenti per segnalarcelo.

[27] https://we.riseup.net/avana/freepto-docs

Siamo una rete di compagni e compagne costituitasi all'indomani degli arresti del **15 ottobre 2011**, uniti dalla volontà comune di non lasciare soli i giovani compagni e le giovani compagne arrestate durante quella giornata di rabbia e rivolta.

Ciascuna e ciascuno di noi è portatore di una propria specificità di pensiero e di azione. Siamo accomunate e accomunati dall'idea che la solidarietà sia un'arma per scardinare l'isolamento, l'indifferenza e la paura che i poteri infondono nelle vite di gruppi e individui.

Siamo consapevoli dell'importanza di sostenere e consolidare relazioni di confronto e condivisione sulle tematiche del controllo, della repressione e della reclusione.

Pensiamo sia opportuno creare e diffondere responsabilità comuni, affinché nessuna persona colpita dalla repressione si senta, né rimanga, sola.

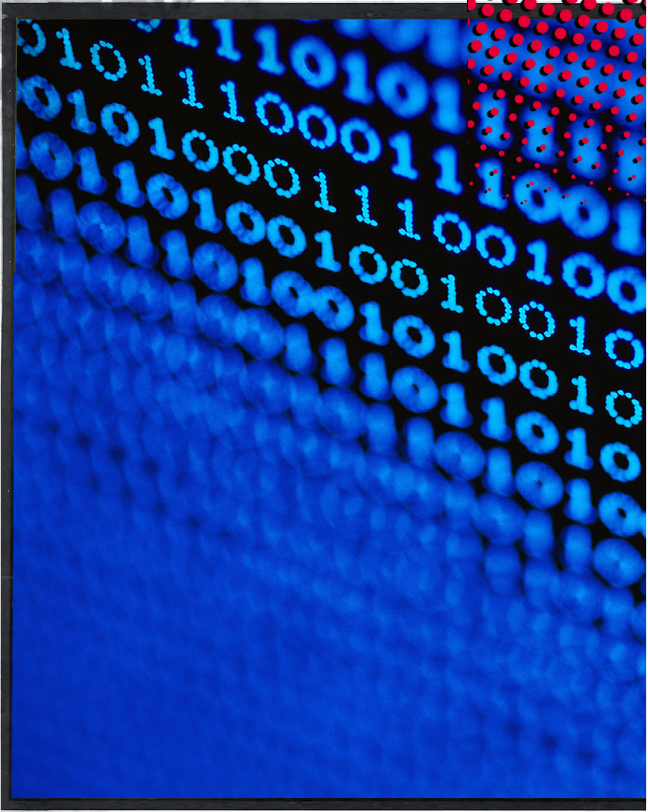
Parlare di repressione digitale, scegliendo di sostenere e diffondere l'opuscolo del collettivo **AvANa**, rientra nel progetto della "rete" di fornire strumenti utili ad evadere il controllo che oggi si manifesta sempre più sotto forma di dispositivi tecnologici.

Conoscere bene le maglie della repressione è l'unico modo per evitare di rimanerci intrappolati.

Se evadere è un istinto naturale per ogni prigioniera e prigioniero che non vuole farsi addomesticare, lottare è una scelta consapevole per rompere le catene dell'oppressione e dello sfruttamento.

libere tutte, liberi tutti!

Evasioni



AVANA
CSOA FORTEPRENESTINO