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 2013.

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.

Questo opuscolo può essere trovato anche su https://we.riseup.net/avana/opuscolo

CHI HA QUALCOSA DA NASCONDERE?

Tutti e tutte.

Sul tuo computer transitano un mare di informazioni potenzialmente delicate: i siti che visiti, le persone con cui parli, le informazioni che ti scambi possono essere oggetto di indagine. Possono addirittura essere raccolti in modo sistematico per meglio "classificarti". Con un po' di analisi è possibile sapere chi sei, dove vivi, la tua routine, il tuo "carattere", la tua faccia e quella dei tuoi amici.

In alcuni casi, poi, il computer si può trasformare in una vera "cimice" sfruttando la webcam e il microfono del portatile.

I MIEI DATI SONO AL SICURO?

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

Il tuo computer *contiene* dei dati. Se non si prendono adeguate precauzioni, questi sono accessibili a chi ne ha il controllo *fisico* (anche solo per un momento in cui viene lasciato incustodito) oppure *software* (ovvero penetrando nel computer da remoto, tipicamente tramite internet).

Il tuo computer *comunica* con altri server: chatti, videochiami, scrivi e-mail, ti connetti a dei social network, invii foto, ascolti musica. Qualcuno potrebbe "ascoltare" queste comunicazioni in modo simile a un vicino di casa che origlia dal muro.

Molti dei *servizi* che usi su internet controllano nella pratica i tuoi dati; stai quindi delegando la loro gestione. Ti fidi di loro? 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.

Per finire, ricorda che la gestione della tua sicurezza è principalmente un approccio mentale, in molte occasioni (anche quando non stai usando il computer) è necessaria molta attenzione: ad esempio nell'usare i computer altrui, o quelli di un internet point, potresti lasciare le tue password su quei computer, permettendo ai visitatori successivi di vedere i tuoi dati.

CON I PIEDI PER TERRA

Domanda naturale è chiedersi quanto realistici siano questi problemi, e chi è materialmente in grado di compiere degli attacchi informatici per impadronirsi dei tuoi dati. Alcuni attacchi sono facili per alcuni e difficili per altri.

Ad esempio un collega invadente potrebbe leggere le tue email mentre vi assentate per una pausa, ma difficilmente potrebbe sequestrare il vostro computer casalingo. La polizia solitamente opta per la seconda possibilità, a meno che non riesca a spiarvi mentre siete in bagno, salvo poi trovarsi nella condizione di dover decifrare le vostre mail se siete stati intelligenti e le avete criptate. Situazioni diverse quindi, a seconda del tipo di attacco del quale si diventa bersaglio.

Malware

Tutti sappiamo cos'è un virus.
È possibile usare dei programmi simili a dei virus con lo scopo di ottenere il controllo del vostro computer.
Questa tecnica è sempre più usata dalle polizie di tutto il mondo. C'è qualche evidenza di uso anche da parte della polizia italiana.

È decisamente la tecnica più potente; **ci si può proteggere solo evitando di utilizzare Micro$oft Windows**.

Continua online su:
https://we.riseup.net/avana/malware-di-stato

Richiesta di dati al fornitore di servizi

Tutti i servizi che utilizzi sono online: email, social network.

La polizia può chiedere (anche senza mandato) alle aziende che gestiscono i servizi che utilizzi, tutto ciò che è possibile sapere su una certa email o su uno specifico account: solitamente i contenuti delle comunicazioni e gli indirizzi IP da cui l'utente si è collegato.

A volte non basta neanche cancellare le informazioni sui nostri account online per stare al sicuro, ad esempio: Facebook (e forse anche altre aziende) mantiene nei propri server, per un certo periodo di tempo, una copia dei dati che l'utente ha cancellato dal suo account; GMail "scoraggia" la cancellazione delle email (ed inoltre mentre tu stai pensando di cancellare le mail, queste vengono in realtà archiviate).

Intercettazione

Il tuo provider (fastweb, alice, tiscali, infostrada, etc) ha il controllo sui dati che attraversano la tua connessione.
Alcuni di questi dati sono “cifrati”, ed è quindi molto complicato leggerne il contenuto, ma molti altri invece viaggiano in chiaro.
In sostanza, una buona parte delle tue comunicazioni è perfettamente leggibile dall’azienda che ti fornisce la connessione alla rete.

Il tuo fornitore di ADSL o di telefonia mobile potrebbe collaborare con la polizia permettendole di controllare ciò che fai, una pratica, a quanto pare (ancora) molto diffusa in italia, ma altrove lo è molto di più, e senz’altro meno potente di quella del malware, visto che con qualche accortezza la si può prevenire.

Dal punto di vista legale, questo procedura è del tutto equivalente alla “intercettazione telefonica”, con la differenza che i dati vengono chiesti al vostro provider (ovvero chi vi fornisce la connessione internet) anche se in molti casi quest’ultimo coincide col vostro gestore telefonico.

Sequestro

Con un mandato, la polizia può sequestrare del materiale informatico a scopo di indagine.

Dopo il sequestro, la polizia prende possesso di tutto ciò che trova su computer e hard disk, incluse quindi le password che avete salvato sul vostro browser, ad esempio, i vostri documenti, la cronologia (del browser, delle chat, etc.) e, se usate un client di posta, delle vostre mail.

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

LEGAL

La perquisizione informatica

Come funziona

Se vi trovate in un luogo pubblico è possibile per la polizia chiedere di controllare il vostro computer (o smartphone) per cercare elementi.

Come comportarsi

Per quanto riguarda il portatile, una semplice soluzione è abbassare lo schermo: la maggior parte dei sistemi a quel punto chiede una password per sbloccare l'accesso al sistema operativo. Se non è troppo facile (ad esempio uguale al nome utente) difficilmente sarà possibile accedere al sistema con una semplice perquisizione. Ricordate che non siete tenuti 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 momento del sequestro

Il caso del sequestro è differente: si tratta tipicamente di un'evento più organizzato, in cui la polizia entra in un domicilio con un mandato per sequestrare alcuni oggetti, tra cui il computer.

Continua online su
https://we.riseup.net/avana/opuscolo-legal

RICETTE PER LA TUA SICUREZZA

Abbandonare windows

Installare GNU/Linux su pc in cui c'è già Windows
Difficoltà di configurazione: media

Installare solo GNU/Linux
Difficoltà di configurazione: facile

Difficoltà quotidiana: media

Utile contro: malware + intercettazioni

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, perchè permette l'accesso completo al nostro computer e di conseguenza anche a tutti i nostri dati.

Inoltre, dopo l'analisi di alcuni malware è emerso che questi permettono a chi ne ha il controllo (ad esempio la Polizia) di utilizzare da remoto il computer come una vera e propria microspia.

L'utilizzo di malware come strumento di intercettazione si sta lentamente diffondendo e generalmente il target più vulnerabile a questo tipo di attacco è il sistema operativo Micro$oft Windows. Non sono noti invece virus per GNU/Linux o per Mac OS X.

Il rimedio migliore per proteggersi da questo genere di attacco è abbandonare Windows a favore di un sistema operativo open source come GNU/Linux.
Ad esempio puoi usare **FREEPTO** (vedi l'ultimo capitolo per maggiori informazioni).

Cifrare i propri dati

SE DEVI INSTALLARE DA ZERO O SU MAC
DIFFICOLTÀ DI PREPARAZIONE: FACILE

IN TUTTI GLI ALTRI CASI
DIFFICOLTÀ DI PREPARAZIONE: MEDIO/DIFFICILE

DIFFICOLTÀ QUOTIDIANA: FACILE

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 password all'avvio del computer. Se la password viene tenuta segreta, il contenuto del disco sarà indecifrabile.

NOTA: 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 e-mail con Thunderbird, tenendole via dai server di posta e custodirle al sicuro sul vostro disco cifrato.

Questo non vi protegge però dai malware: per evitarli, il consiglio migliore che possiamo darti è **abbandona Windows**.

Continua online su
https://we.riseup.net/avana/opuscolo-crypto

Gestione password

Difficoltà di configurazione: nessuna
Difficoltà quotidiana: facile
Utile contro: accessi non autorizzati

Una password "sicura" aiuta a prevenire (possibili) accessi al vostro account da parte di terzi. Spesso, per pigrizia, si imposta una stessa password per accedere a più servizi in rete. Inoltre, password semplici possono essere indovinate da programmi che "provano ogni possibile combinazione".

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 fidate "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 **MaIuSC0l3** e minuscole, combina numeri e simboli. Lunghezza minima consigliata: 8 caratteri.*

- Non condividere le password se non e' proprio necessario.

Usa Firefox + HTTPS Everywhere

DIFFICOLTÀ DI CONFIGURAZIONE: FACILE
DIFFICOLTÀ QUOTIDIANA: NESSUNA
UTILE CONTRO: INTERCETTAZIONE

Le comunicazioni su internet possono essere cifrate (ovvero leggibili solo dal mittente e dal destinatario) o in chiaro (ovvero leggibili da chiunque).

In molti casi è possibile utilizzare comunicazioni cifrate,

ma il nostro browser (come Firefox) non lo fa in automatico. 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 sicurezza: le intercettazioni delle comunicazioni cifrate sono infatti molto difficili, e possono essere condotte solo da attaccanti molto motivati.

Continua online su
https://we.riseup.net/avana/opuscolo-https

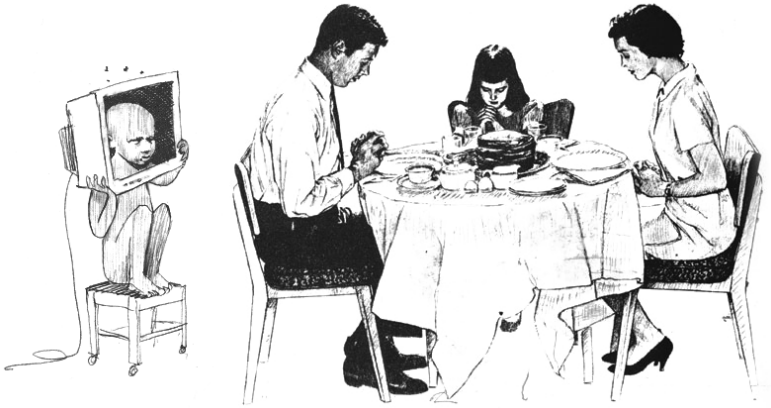
Cancellazione sicura dei file

Difficolta' di configurazione: facile
Difficolta' quotidiana: facile
Utile contro: sequestro del computer

Quando cancelli i dati sul tuo PC ne 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 su
https://we.riseup.net/avana/opuscolo-wipe

COMUNICARE



Usare servizi autogestiti

Difficolta' di configurazione: facile
Difficolta' quotidiana: facilissima
Utile contro: Identificazione, Richiesta dati al fornitore di servizi

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 (ma hanno un costo per chi li fornisce: sostienili con benefit e donazioni!)

I servizi autogestiti (riseup.net, autistici.org, indivia.net) 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; molti servizi commerciali ti incentivano ad abbinare un numero di cellulare ad un account, nessun server autogestito di dirà mai di fare cose simili).
Per richiedere, ad esempio, una email su autistici.org vai su services.autistici.org e compila il modulo. Dopo qualche giorno la tua email verrà attivata.

Continua online su
https://we.riseup.net/avana/opuscolo-servizi

Chat sicura

Difficolta' di configurazione: media
Difficolta' quotidiana: media
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 cuurioso di leggere facilmente le tue conversazioni.
Questo tipo di "protezione" non ti protegge contro altre minacce perchè delega completamente alle aziende la protezione della tua privacy.
Non c'è alcun buon motivo per credere che di fronte alla richiesta della magistratura queste aziende intraprendano delle azioni per la tutela della tua privacy.

Esistono però delle soluzioni:

I server autogestiti **A/I** e **Riseup** offrono ai loro utenti **Jabber (XMPP)**, uno strumento di Instant Messagging che è amico della tua privacy.
Peraltro il servizio è attivo di default per chiunque abbia già una mail con loro.
Inoltre, per migliorare notevolmente la tua privacy, puoi utilizzare **OTR**, una tecnologia che permette, in maniera semplice, la cifratura di tutte le tue conversazioni: con **OTR** puoi stare sicuro che nemmeno **A/I** è in grado di leggere le tue conversazioni e che nessuno ti sta intercettando.

Continua online su
https://we.riseup.net/avana/opuscolo-im

Usa GPG con Thunderbird + Enigmail

Difficolta' di configurazione: media
Difficolta' quotidiana: media
Utile contro: Intercettazione

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

Anche se usi servizi più fidati, come **Autistici/Inventati**, **Riseup**, **Indivia** o **Ortiche**, non è comunque una buona pratica di sicurezza quella di mandare email leggibili da 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**.

Continua online su
https://we.riseup.net/avana/opuscolo-gpg

ANONIMATO 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 e questi dati possono essere utilizzati successivamente per identificare, ad esempio, l'autore di un contenuto pubblicato su Internet.

Per questo motivo non è sufficiente utilizzare uno pseudonimo per proteggere, ad esempio, la nostra reale identità sui social network.

Esistono software che ci danno la possibilità di rimanere anonimi durante la navigazione con il browser su internet:

TorBrowser

DIFFICOLTÀ DI CONFIGURAZIONE: FACILE
DIFFICOLTÀ QUOTIDIANA: FACILE
UTILE CONTRO: IDENTIFICAZIONE + INTERCETTAZIONI

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, che ti permette di far 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.

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-TORBROWSER

VPN autistici/riseup

DIFFICOLTÀ DI CONFIGURAZIONE: MEDIA
DIFFICOLTÀ QUOTIDIANA: FACILE
UTILE CONTRO: IDENTIFICAZIONE + INTERCETTAZIONI

Una *VPN* permette di proteggere il flusso di dati prodotto dalla tua navigazione inserendolo in una sorta di tunnel virtuale cifrato. 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 che permette di proteggere il proprio anonimato in rete.

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-VPN

Googlesharing

GoogleSharing è un plugin per Firefox facile da utilizzare, gratuito e libero (Open Source) che permette di anonimizzare le tue ricerche su Google.
Quando fai una ricerca, Google colleziona informazioni che possono identificarti. Viene registrato l'indirizzo dal quale la ricerca viene effettuata ed i contenuti della ricerca stessa. Probabilmente Google saprà molto più delle tue ricerche di te stesso!
GoogleSharing devia tutto il traffico relazionato a Google attraverso un server separato (gestito dagli attivisti di Riseup.net), in modo completamente trasparente (non devi far altro che installare il plugin).
Come risultato le tue attività online veranno aggregate con quelle di tutti gli altri utenti che usano questo plugin, rendendo le informazioni un polpettone difficilmente utilizzabile da terzi.
https://we.riseup.net/avana/opuscolo-googlesharing

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-GOOGLESHARING

SICUREZZA DEL TUO SMARTPHONE

Gli smartphone sono estremamente difficili da gestire in maniera sicura.

Spesso la localizzazione attraverso la rete GSM rappresenta una prova usata nei processi per dimostrare la partecipazione degli attivisti ad un evento.
Inoltre, gli smartphone moderni possono tracciare accuratamente i nostri spostamenti attraverso il sistema satellitare GPS.

Come se non bastasse è possibile sviluppare malware che trasformano gli smartphone in strumenti di intercettazione altamente tecnologici.

Per tutte queste ragioni **è fortemente sconsigliato utilizzare gli SmartPhone in situazioni dove il rischio di azioni repressive è molto alto**.
Con l'accusa di "devastazione e saccheggio" abbiamo visto condannare attivisti per il semplice fatto di essere "nei pressi" di dove è avvenuto un fatto. Bisogna rendersi conto della situazione nella quale ci troviamo e capire quanto è rischioso avere con noi uno strumento che segnala continuamente la nostra posizione.

Se è veramente necessario comunicare telefonicamente durante un corteo particolarmente rischioso, il consiglio che possiamo darvi è: utilizzate un vecchio telefono ed una sim anonima (vendute senza la richiesta di un doccumento di identità).

In ogni caso esistono strumenti che possono rendere più sicuro l'uso degli smartphone in scenari meno critici:

ObscuraCam: anonimizzare le immagini

Difficoltà di configurazione: facile
Difficoltà quotidiana: 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 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.

Obscuracam è un'applicazione per Android che rende semplicissima questa operazione e ti permette di editare velocemente le foto prima di pubblicarle online.

Continua online su
https://we.riseup.net/avana/opuscolo-obscuracam

Gibberbot: Chat sicura

Difficoltà di configurazione: facile
Difficoltà quotidiana: facile
Utile contro: intercettazioni

Gibberbot è un client Jabber per android che supporta nativamente sia OTR (quindi ti permette di cifrare le tue comunicazioni) sia Tor (nella versione per Android chiamata Orbot).
In alcune situazioni può tornare utile utilizzare il tuo account Jabber, ma anche in questo caso valgono le avvertenze relative all'insicurezza intrinseca degli smartphone.

Continua online su
https://we.riseup.net/avana/opuscolo-gibberbot

Ostel: cifrare le telefonate VoIP

Difficoltà di configurazione: facile
Difficoltà quotidiana: facile
Utile contro: intercettazioni

L'intercettazione delle telefonate su rete GSM comprende circa il 95% di tutte le tipologie di intercettazione che vengono effettuate in Italia.
Non è quindi per nulla scontanto ribadire che usare il telefono può essere molto rischioso.
L'utilizzo della rete telefonica GSM può sia mettere a rischio la riservatezza delle nostre conversazione sia offrire dettagliate informazioni utili alla nostra localizzazazione (la triangolazione

con le celle GSM è un metodo usato spessissimo durante i processi).
Non esistono strumenti opensource che permettono di cifrare le conversazioni su rete GSM, è però possibile utilizzare degli strumenti che permettono di cifrare le conversazioni su rete VoIP.
Senza mai dimenticare l'insicurezza intrinseca dei dispositivi smartphone **(è sempre meglio vedersi di persona e in un luogo sicuro)** è possibile cifrare le nostre conversazioni utilizzando OsTel un software VoIP open source.

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-OSTEL

TextSecure

DIFFICOLTÀ DI CONFIGURAZIONE: MEDIA
DIFFICOLTÀ QUOTIDIANA: FACILE
UTILE CONTRO: INTERCETTAZIONI, PERQUISIZIONI

TextSecure, sviluppato dal Whisper Systems e raccomandato da Guardian Project, è un'applicazione opensource che fornisce un robusto sistema di cifratura per gli SMS del tuo telefono.
È utile ad evitare che il contenuto dei messaggi sia accessibile dal vostro gestore telefonico o dalla polizia durante il normale utilizzo oppure dopo un sequestro.

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-TEXTSECURE

Carte telefoniche prepagate

Difficoltà di configurazione: facile
Difficoltà quotidiana: facile
Utile contro: intercettazioni

In alcune 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 è 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:

- **Usare il "private browsing"** (anche detto Incognito Mode in google chrome), una modalità in cui la cronologia e le password non vengono salvate.

CONTINUA ONLINE SU
HTTPS://WE.RISEUP.NET/AVANA/OPUSCOLO-PRIVATE

- **Fare logout** dai tuoi account, altrimenti il successivo utilizzatore del computer avrà accesso ai tuoi dati!

- **Ricordarsi 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, ecc.). È molto difficile proteggersi da questo tipo di attacchi, ma alcuni suggerimenti sono:

- 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).

per scaricare Freepto e ulteriori info:
https://avana.forteprenestino.net/freepto

Quali sono le caratteristiche principali di Freepto?

Pensata per gli attivisti.

Esistono molte distribuzioni GNU/Linux orientate alla sicurezza ed alla privacy, **TAILS** è forse la più famosa di questo genere di distribuzioni.

Queste distribuzioni sono chiamate "live" ovvero offrono un sistema operativo "pulito" ogni volta che le utilizziamo, perchè 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 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 oeprativo 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.

***Truecrypt**, per gestire archivi cifrati.*

***Torbrowser-launcher**, 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.*

Personalizzabile

Lo sviluppo di **freepto** è basato su **Debian Live Build**, un insieme di tool che permettono di generare delle distribuzioni live personalizzate basate su Debian.

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**:

HTTPS://GITHUB.COM/AVANA-BBS/FREEPTO-LB

Come si usa?

A questa pagina abbiamo raccolto la documentazione e qualche piccolo tutorial su come configurare **freepto**:

HTTPS://WE.RISEUP.NET/AVANA/FREEPTO-DOCS

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

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 sottoforma 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