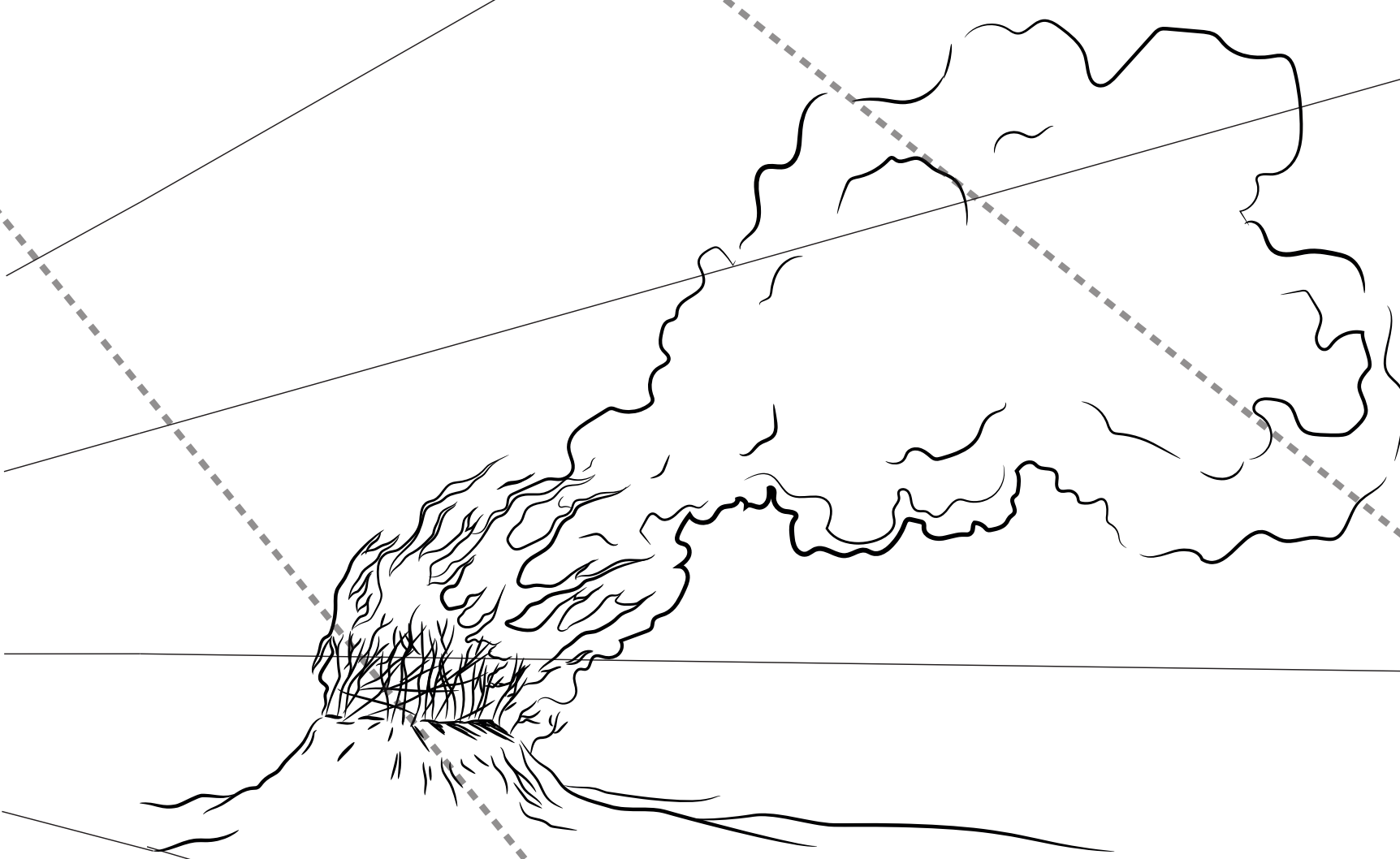
MANUALE DI CURA COLLETTIVA

& / AUTODIFESA DIGITALE



US AND THEM

Co-funded by the European Union

Maghweb

crisis

[EdIPo]
Equipo de Investigación Política

vi invitiamo ad adattare ciò che vi serve al vostro contesto.
Se la quantità di informazioni è eccessiva,
prendete ciò che vi serve e diffondete il resto

UN INVITO A RIFLETTERE SU LEGAMI E ABITUDINI

come sono i territori che attraversiamo e con i quali ci relazioniamo?

quali tracce lasciamo quando li attraversiamo?

non esiste la bacchetta magica.
Riflettere in maniera attiva sulle nostre abitudini quotidiane nel mondo virtuale, adottare uno sguardo attento, vigile e aperto basato sulla cura reciproca al fine di costruire nuove abitudini, pianificare e attuare azioni preventive

richiede tempo e spazio

Però non è un viaggio solitario,
ma un processo condiviso di apprendimento continuo:
il suo successo dipende dalla nostra capacità di renderlo collettivo

se l'impotenza paralizza, farci delle domande, mettere in discussione le consuetudini, scambiarci esperienze nella ricerca di strumenti, ci permette di allargare i nostri orizzonti

~~SICUREZZA~~ CURA

~~STATO~~ PROCESSO

~~INDIVIDUO~~ COLLETTIVO

Il modello di business che si cela dietro le nostre interazioni quotidiane non può essere ignorato. Ci troviamo in un ecosistema che estrae dati, governato da poche mega-aziende, dove le informazioni sono sottoposte a un regime di valorizzazione, speculazione e manipolazione.

STRATEGIE DI RESISTENZA

RIDURRE_DIMINUIRE LE TRACCE CHE LASCIAMO

OSCURARE_CONFONDERE E MOLTIPLICARE LE NOSTRE IDENTITÀ ONLINE

DIVIDIRE_OGNI COSA AL SUO POSTO/SEPARARE I PROFILI

RAFFORZARE_I DISPOSITIVI DI PROTEZIONE

PRIMA LINEA DI DIFESA

Non esistono strumenti tecnologici in grado di sostituire le pratiche analogiche: EVITIAMO L'OVER SHARING. Forniamo solo le informazioni personali o sensibili assolutamente necessari e quando è possibile, utilizziamo diversi account o dati.

CHE INFORMAZIONI FORNIAMO QUANDO NAVIGHIAMO IN RETE?

LA LOCALIZZAZIONE
rivelata dall'IP assegnato o dall'accesso alla nostra posizione GPS

IL CONTENUTO
delle nostre comunicazioni

LE INFORMAZIONI
sensibili o personali

LA RETE DI CONTATTI
con cui interagiamo

MODELLO DA (DIS)INNESCARE

prendiamoci una pausa per riflettere insieme sul nostro punto di vista

DOMANDE GUIDA PER OPERARE UNA VALUTAZIONE DEI RISCHI

Esempi
canali di comunicazione del collettivo; dati personalidei membri; dati della comunità che ci segue o che partecipaagli eventi

COSA vogliamo proteggere?

Quali ***MINACCE*** dobbiamo affrontare?

Esempi
furto della password tramite phishing; bullismo e molestie; accesso non autorizzato ai dispositivi; furto d'identità sui social media; monitoraggio o sorveglianza da parte del governo; intercettazione delle comunicazioni

Esempi
Da un ex partner; attacchi generalizzati e casuali; aziende pubblicitarie; server e provider che conservano tutti i dati di navigazione non criptati

Da **dove** provengono?

Quanto è probabile che accada
e quanto è grave se accade?

Quali risorse abbiamo per difenderci?

Non pretendiamo di essere sempre attent3, ma di sviluppare comportamenti consapevoli e concreti di riduzione del danno basati sui nostri rischi, capacità, bisogni e priorità

Identificare le minacce e classificarle in base alla probabilità e al danno che possono arrecarci consente di tarare più efficientemente le azioni di mitigazione dei rischi.

MINACCIA	PROBABILITÀ 1-molto bassa 5-molto alta	DANNO 1-lieve 5-molto grave	MITIGAZIONE che possiamo fare?	IMPEDIMENTI E OSTACOLI
Furto della password tramite *phishing* - truffa virtuale attraverso link falsi -	*3*	*5*	*Integrare fattori di autenticazione; utilizzare un'app per la gestione delle password; stare attent3 ai link che riceviamo*	*Tempo e disponibilità a rafforzare la sicurezza delle password e degli accessi*

STRUMENTI per l' AutoDifesA

Non rappresentano una soluzione risolutiva nè definitiva

✓open source ✓gratis

ProtonDrive

8 Servizio di archiviazione online criptato con un massimo di 1GB per account.

CryptPad

4 Spazio di collaborazione online che permette di lavorare su fogli di calcolo, documenti di testo, kanban, moduli e diapositive.
Offre uno spazio di archiviazione online criptato fino a 1 GB

Tails

Sistema operativo parallelo portatile di natura anonima e anmesica. Offre una selezione di strumenti per lavorare con informazioni sensibili e comunicazioni sicure.

RiseUp Pad

5 Consente la creazione di documenti collaborativi online, con la possibilità di proteggerli tramite password e programmarne l'autodistruzione.

ProtonMail

9 Posta elettronica con crittografia end-to-end

VeraCrypt

7 Strumento per criptare dischi e cartelle su computer e pendrive.

KeePass

6 Strumento per la gestione sicura di password diverse, tramite un'unica master password.

Wormhole

3 Consente la condivisione di file fino a 10GB con crittografia end-to-end tramite link con scadenza automatica.

V.P.N.

1 Rende anonimo il luogo di connessione e riesce a criptare il traffico dati (consigliamo Riseup VPN)

Tor

2 Riesce a criptare tre volte il traffico dati e lo reindirizza attraverso server random della rete Tor per nascondere l'origine e la destinazione del traffico dati. Blocca il tracciamento e l'accesso ai contenuti di navigazione a terzi

Nessuno di questi strumenti é utile se non é aggiornato

Nessuno strumento è infallibile o garantisce al 100% l'anonimato su Internet, ma ognuno di essi fornisce diversi livelli di protezione. Gli strumenti, così come i rischi, sono soggetti a cambiamento ed è bene quindi mantenersi sempre informat3. Si consiglia di aggiornare regolarmente sistemi operativi e software, così come le proprie valutazioni e strategie.

NAVIGAZIONE

1- VPN: https://riseup.net/en/vpn

Rende anonimo il luogo di connessione e riesce a criptare il traffico dati. Aggira la censura ed evita il tracciamento finalizzato alla sorveglianza o pubblicità. Come? Una connessione criptata incanala il vostro traffico dati attraverso i suoi server sicuri verso l'internet pubblico, come se fosse un tunnel. Consigliamo RISE UP VPN perché è gratuita e non registra gli indirizzi IP (deve però essere attivata ad ogni utilizzo), inoltre è disponibile anche per Android (alternative ProtonVPN, NordVPN, Tunnel Bear).

2- TOR: https://www.torproject.org/download

Riesce a criptare tre volte il traffico dati e lo reindirizza attraverso server random della rete Tor per nascondere l'origine e la destinazione del traffico dati. Blocca il tracciamento dati e rende invisibile il contenuto della tua navigazione a terzi. TOR riesce a criptare e rendere anonimo il tuo traffico, passandolo attraverso tre livelli. I livelli sono server gestiti da diverse persone e organizzazioni in tutto il mondo. Tor evita che qualcuno veda la tua connessione a internet e sappia quali sono le tue attività online.

Sono state rilevate vulnerabilità in alcuni dei suoi nodi di uscita, pertanto si consiglia di aggiungere un ulteriore livello di protezione combinando il suo utilizzo con una VPN.

COLLABORAZIONE

3- WORMHOLE: https://wormhole.app/

Con crittografia end-to-end e link con scadenza automatica per l'invio di file fino a 10 GB. Il cloud rimane online per massimo 24 ore e poi si autodistrugge.

4- CRYPTPAD: https://cryptpad.fr/

Spazio di collaborazione online, con crittografia end-to-end, che permette di lavorare su fogli di calcolo, documenti di testo, kanban, codici, formulari, lavagne e diapositive fino a un massimo di 1GB. Attenzione! Se dimentichi la password, non è possibile recuperarla.

5- PAD RISE UP: https://pad.riseup.net/

Consente la creazione di documenti collaborativi online, su server sicuri, con la possibilità di proteggerli tramite password e programmarne l'autodistruzione. Inoltre, funziona come alternativa per chattare senza necessità di utilizzare altre app.

CUSTODIRE LE INFORMAZIONI

6- KeePass: https://keepassxc.org/

Strumento per la gestione sicura di tutte le tue password, senza doverle ricordare, accedendovi tramite un'unica master password. Genera inoltre password sicure.

7- VERACRYPT: https://www.veracrypt.fr/

Può criptare i tuoi hard-disk e cartelle "a riposo" per evitare l'intrusione di terzi.

COMUNICAZIONE

8- PROTONDRIVE: https://proton.me/drive

Mette a disposizione 1 GB di spazio di archiviazione criptato in un cloud online.

9- PROTONMAIL: https://proton.me/mail

Posta elettronica con crittografia end-to-end.

10- JITSI MEET: https://meet.jit.si/

Software gratuito per videoconferenze, open source e con crittografia end-to-server/transit (crittografia dal dispositivo al server, dove viene decifrata e poi criptata nuovamente per l'invio a destinazione). Non richiede registrazione.

11- EMAIL USA E GETTA:

https://temp-mail.org/en e **https://www.guerrillamail.com**

Indirizzi email temporanei per nascondere l'identità, senza necessità di registrazione.

RICERCA DI INFORMAZIONI

12- DUCKDUCK GO: https://duckduckgo.com/

Motore di ricerca che non registra il traffico dati e non orienta commercialmente i risultati in funzione del profilo dell'utente..

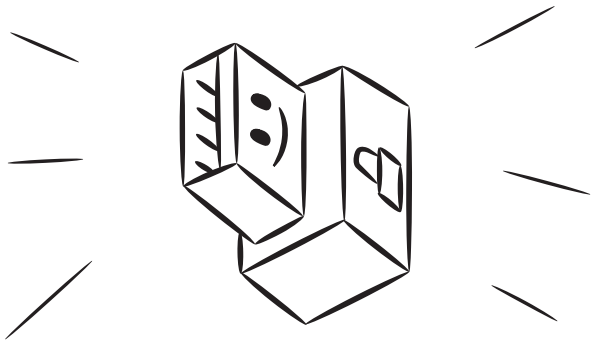
La tutela della propria sicurezza non dipende solo dagli strumenti: l'anello debole è spesso rappresentato dalle pratiche dell'utente piuttosto che dai dispositivi. Anche se utilizziamo strumenti sofisticati, la fuga di informazioni è sempre possibile.

Tails

È un sistema operativo portatile che ti protegge dalla sorveglianza e dalla censura

È indipendente, si può inserire in una pendrive e utilizzare da qualsiasi computer

- ✓ **EVITA IL TRACCIAMENTO**
- ✓ **SOFTWARE LIBERO**
- ✓ **MASSIMA SICUREZZA GRATIS**



Non lascia tracce nel computer

Basta una chiavetta USB per attivare Tails

Archivio persistente

Puoi salvare alcuni dei tuoi file in un volume persistente

Amnesia

Tutto sparisce automaticamente quando arresti Tails

Attrezzatura

Offre applicazioni per lavorare su documenti sensibili e comunicare in maniera sicura

- Tor Browser con uBlock, un browser sicuro con una funzione integrata per il blocco della pubblicità
- Thunderbird, per mail cifrate
- KeePassXC, per creare e conservare password sicure
- LibreOffice, una suite di app da ufficio
- OnionShare, per condividere file attraverso Tor
- App per rimuovere i metadati

https://tails.boum.org

TUTTO PRONTO PER NAVIGARE CON UNA CONFIGURAZIONE PREDEFINITA SICURA

Per evitare errori:

- *Le applicazioni vengono bloccate automaticamente se cercano di connettersi a Internet senza Tor.*
- *Tutti i file che si trovano nell’archivio persistente sono cifrati automaticamente.*
- *Tails non scrive nulla sul disco fisso. L'intera memoria viene cancellata all'arresto.*

raccomandazioni

- Controllare accessi e password condivise con Google e altre app: chi ha accesso alle mie password? Alla mia posizione, foto, connessioni e contatti?

- Pulire l'identità virtuale: eliminare account e applicazioni che non usi, così come foto, messaggi e email che non ti servono più.

- Interrompere l'emissione di segnali (bluetooth, wifi, GPS) e coprire le webcam quando non le utilizziamo. Allontanare il telefono per evitare intromissioni di terzi in contenuti sensibili.

- Diffidare dei link inaspettati, anche se conosciamo il mittente. Controlla sempre prima di aprirli.

- Quando è possibile, attiva l'eliminazione automatica dei messaggi e scegli canali di comunicazione che possano criptare l'informazione nel traffico (end-to-end).

- Cambia le vecchie password, non usare la stessa password per più account e aumenta i fattori di autenticazione.

È importante ricordare che tutto ciò che viene caricato su internet rimane archiviato anche se l'utente lo cancella o lo nasconde.

È consigliabile fare una pulizia per diminuire i rischi in caso di attacchi hacker, però è importante ricordare che le informazioni non scompaiono, rimangono online per sempre

CRITERI PER PASSWORD SICURE

- Lunga (meglio una frase)
- Senza dati personali
- Cambiarla spesso
- Non utilizzarla più volte, nemmeno variandola leggermente
- Doppio fattore di autenticazione

IDEALE

Utilizzare un gestore di password che le generi automaticamente, ti richieda di cambiarle e le custodisca criptate al di fuori del browser.

Quanto è sicura la mia password?

https://www.security.org/how-secure-is-my-password

Come sapere se ho subito un attacco hacker o c'è stato un data leak?

https://haveibeenpwned.com

US AND THEM

Co-funded by
the European Union

maghweb

crisis

[EdIPo]
Equipo de Investigación Política

Giugno 2023