PROTOCOLLO DI SICUREZZA DIGITALE

una guida di sicurezza di base per tutti

internationalistcommune.com

Protocollo di Sicurezza Digitale

una guida di sicurezza di base per tutti

internationalistcommune.com

Protocollo Informativo di Sicurezza Digitale

Usiamo i nostri telefoni, tablet o smartphone, così come i nostri computer e le nostre fotocamere ogni giorno. Pertanto, la nostra sicurezza quando li usiamo è un argomento molto importante che dobbiamo affrontare. Soprattutto per le persone che si organizzano e lottano contro il sistema capitalista, la sicurezza e l'autodifesa sono argomenti essenziali che dovrebbero essere presi in considerazione anche a livello digitale. Con l'uso quotidiano di questi dispositivi possiamo diventare vulnerabili allo stato o a chiunque altro voglia attaccarci. Quando riceviamo una chiamata, quando usiamo Internet, quando mandiamo messaggi, lasciamo tracce digitali che il nemico può usare contro di noi. **Questo protocollo ha lo scopo di presentare le principali minacce e proporre soluzioni con risorse per adattarsi e proteggersi in modo efficace.**

Sicurezza Digitale per cosa?

Per quanto riguarda la sicurezza digitale, è importante porre alcune domande per capire il motivo per cui determinate misure devono essere adottate per la nostra protezione e l'impatto che hanno. In questo modo possiamo evitare di diventare paranoici o un facile bersaglio per il nemico. Le seguenti domande sono quindi importanti per noi.

Perché è importante prendersi cura della nostra sicurezza?

Proteggere te stessa/o, i tuoi dispositivi, telefono e computer significa proteggere allo stesso tempo le tuoe compagne/i, il tuo collettivo o la tua organizzazione. La sicurezza informatica non è una questione individuale e siamo responsabili non solo della nostra sicurezza ma anche di quella delle nostre compagne/i.

Quali informazioni voglio proteggere?

La mia identità, le mie ricerche su Internet, la mia attività sui social network, in generale la mia posizione o la mia presenza in un determinato luogo, le mie comunicazioni, i canali di informazione, le pubblicazioni su Internet...

Da chi voglio proteggermi, da quali nemici?

Persone sconosciute, servizi di intelligence statali, altri stati, banchieri, hacker, servizi di polizia giudiziaria, ladri, il mio operatore di telefonia mobile o il mio fornitore di servizi Internet, ecc ...

Che tipo di attacchi?

Quando il nemico ha accesso diretto al mio telefono dopo everlo cercato e sequestrato, quando il nemico mi sta cercando su Internet, quando un nemico cerca di hackerare il mio computer, quando il mio nemico chiede informazioni al mio operatore telefonico ...

Vogliamo capire meglio tutto questo. Cominciamo quindi dalle tracce utilizzabili che lasciamo sui nostri dispositivi (telefono/computer) e poi diamo un'occhiata a quelle che lasciamo durante le nostre connessioni Internet.

Per questo motivo, vedremo come lasciamo tracce sui computer e quali tipi di sistemi operativi (software che gestisce l'hardware e le applicazioni di un computer) esistono e in che modo differiscono tra loro in termini di sicurezza e utilizzo. Faremo lo stesso per i telefoni e capiremo come e perchè utilizzare un VPN (Virtual Private Network). Capiremo quali tipi di attacchi da parte del nemico esistono e come possiamo proteggerci da essi. Ciò significa che vi presenteremoç anche modi di utilizzo sicuro e buone pratiche per i dispositivi con cui lavoriamo quotidianamente.

Computer

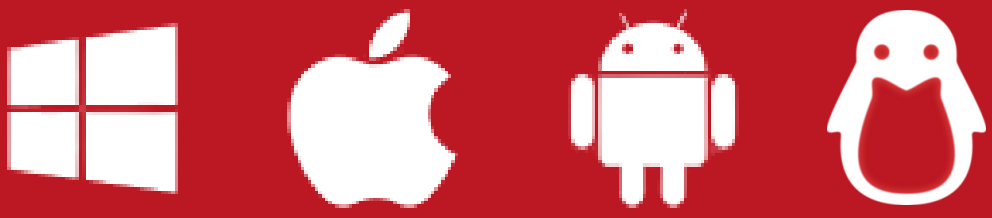
Sui computer lasciamo tracce utilizzabili quando:

- Archiviamo file (video/foto/audio/documenti...) su un disco rigido (interno o esterno), su chiavette USB e su schede SD.

- Ci connettiamo a Internet per visitare siti web, utilizziamo applicazioni connesse (messaggistica, e-mail, applicazioni di gioco e applicazioni multimediali digitali come Instagram ecc.), scaricare file (foto/video/audio/documenti, ecc.)

Sistemi Operativi

Il sistema operativo svolge un ruolo molto importante nel computer, poiché è responsabile del funzionamento coordinato di tutte le parti del computer, come la memoria, il processore e l'archiviazione. Inoltre, il sistema operativo è quello che traduce il linguaggio del computer in un linguaggio comprensibile per noi. Un computer senza sistema operativo è inutile. I software possono essere intesi come facilitatori per svolgere un compito nel computer. Quindi, ad esempio, se avete bisogno di inviare un messaggio, potete installare un'applicazione che invia messaggi. Il software è questa applicazione. Il termine software viene utilizzato per differenziarlo dall'hardware, ovvero dai componenti fisici di un sistema informatico. Esistono diversi sistemi operativi, ma non tutti offrono le stesse possibilità. Alcuni di questi sistemi operativi sono sistemi operativi “open source”. Ciò significa che si tratta di un sistema operativo o di un software sviluppato in modo collaborativo e che è disponibile per chiunque voglia utilizzarlo, modificarlo e distribuirlo.



- Windows:

È un sistema operativo sviluppato dalla società Microsoft che collabora con i servizi statali di tutto il mondo. Può essere utile per utilizzare software privati per la creazione di contenuti (come Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, ecc.). Tuttavia, è impossibile sapere come i dati del computer vengono elaborati dall'azienda. Non fornisce i suoi algoritmi, le sue fonti e non consente la protezione del disco rigido, quindi è abbastanza facile violare la password e accedere ai dati. Essendo un'azienda capitalista, può vendere le informazioni dei suoi utenti agli Stati (come la Turchia) in cambio della possibilità di rendere accessibili i suoi servizi nei paesi dei dipendenti.

- macOS:

È un sistema operativo sviluppato dalla società Apple Inc. Come per Windows, è impossibile sapere come i dati del computer vengono elaborati dall'azienda. Tuttavia, è utile per utilizzare software privati per la creazione di contenuti (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, ecc.). Non fornisce i propri algoritmi (le proprie fonti) e non consente la protezione del disco rigido. È difficile violare la password e accedere ai dati. Apple dichiara di non vendere dati personali a terzi. In quanto forze anticapitaliste, dobbiamo comunque prendere precauzioni e non fidarci di nessuna di queste aziende.

- Linux:

E’ un sistema operativo open source che dispone di diverse suite disponibili (ad esempio Debian, Ubuntu, ecc.).

È stato sviluppato da Linus Torvalds e si basa sui sistemi operativi Unix.

Non è compatibile con l'utilizzo di software privati per la creazione di contenuti (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro ...). Esistono come alternativa tutti i tipi di applicazioni open source che possono essere utilizzate per la creazione di contenuti privati e per qualsiasi altro lavoro come la comunicazione digitale ed altri, in modo sicuro e privato disponibile per questo sistema operativo. Tutti gli algoritmi (le sue fonti) sono accessibili online e regolarmente controllati da persone in tutto il mondo. È possibile crittografare in modo sicuro il disco rigido e qualsiasi altro sistema di archiviazione. Con una buona frase di accesso, è (molto) difficile violare la password. Ciò significa che violarlo è molto costoso in termini di tempo ed energia, e quindi di denaro, per un nemico che vuole appropriarsi dei vostri dati. Inoltre, molte applicazioni utili per la pulizia dei dati e la navigazione (descritte in dettaglio più avanti) sono preinstallate. È il sistema più efficace per evitare malware e virus. Per questi motivi, si consiglia di utilizzarlo al posto di Windows/MacOS.

Qui puoi scoprire di più.
https://ubuntu.com/download/desktop
https://www.linux.org/pages/download/

- TAILS (The Amnesic Incognito Live System):

Si tratta di un sistema operativo sviluppato per garantire un elevato livello di sicurezza e anonimato durante la navigazione in Internet e l'archiviazione dei file. È un sistema live, il che significa che è possibile installarlo su una chiavetta USB o una scheda SD e utilizzarlo su tutti i computer (ma non sui Macbook), senza utilizzare il sistema operativo originale (Windows/Linux...). Pertanto non si lasciano tracce a meno che non si desideri farlo. La sua funzione amnesica (perde tutta la memoria) consente di non conservare nulla sul computer. Si connette a Internet tramite il browser Tor. È raccomandato dalla maggior parte degli whistle blowers (persone pubblicamente o segretamente monitorano le attività all'interno di un'organizzazione) ed è stato finanziato dal Tor Project (https://www.torproject.org/). Basato su una struttura Linux, con una buona frase di accesso, è (molto) difficile violarne la password.

Ecco la sua documentazione e il tutorial per la sua installazione: https://tails.net/

Telefoni

Su un telefono/tablet, lasciamo tracce utilizzabili quando:

-Comunichiamo tramite SMS/chiamate (tramite un operatore telefonico)
- Scattiamo foto/giriamo video/registriamo suoni
- Utilizziamo applicazioni di localizzazione
- Archiviamo file (video/foto/documenti) sul telefono o su una mini scheda SD
- Ci connettiamo a Internet per visitare siti web, utilizzare applicazioni connesse (messaggistica, e-mail, ecc.), scaricare file (foto/video/audio/documenti...)

Esistono diversi sistemi operativi per telefoni, non tutti offrono le stesse possibilità:

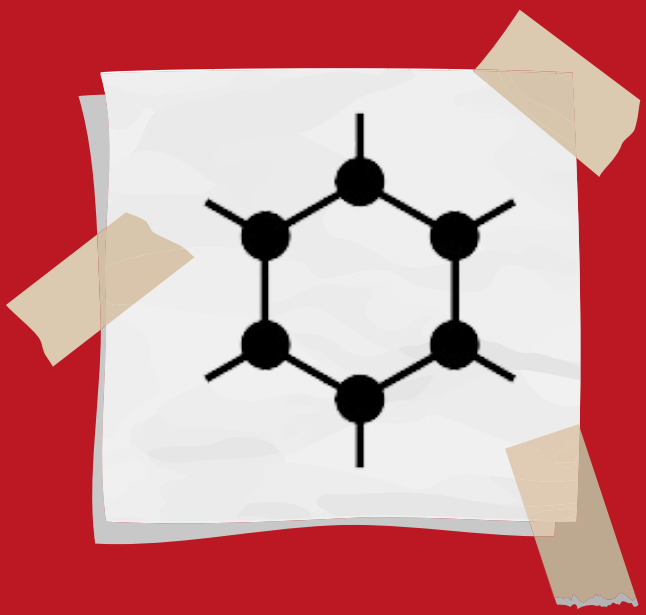
- iOS:
è un sistema operativo mobile per iPhone sviluppato da Apple Inc. È impossibile sapere come vengono trattati i dati del telefono dall'azienda.

- Android:
è un sistema operativo mobile open source utilizzato sulla maggior parte dei telefoni (Samsung, Huawei, Redmi, ecc.). Non offre una buona sicurezza contro l'hacking. È impossibile sapere come vengono trattati i dati del telefono.

- GrapheneOS:

è un sistema operativo mobile open source che supporta solo i telefoni Google Pixel.

Si consiglia di utilizzare la nuova serie Pixel, poiché le serie Pixel precedenti non sono più supportate da GrapheneOS. Questo sistema operativo sostituisce il sistema operativo originale. **Consente di evitare la sorveglianza di Google e di crittografare i contenuti del telefono utilizzando un sistema sviluppato dai compagni.** È compatibile con la maggior parte delle applicazioni Android e offre anche alternative open source.

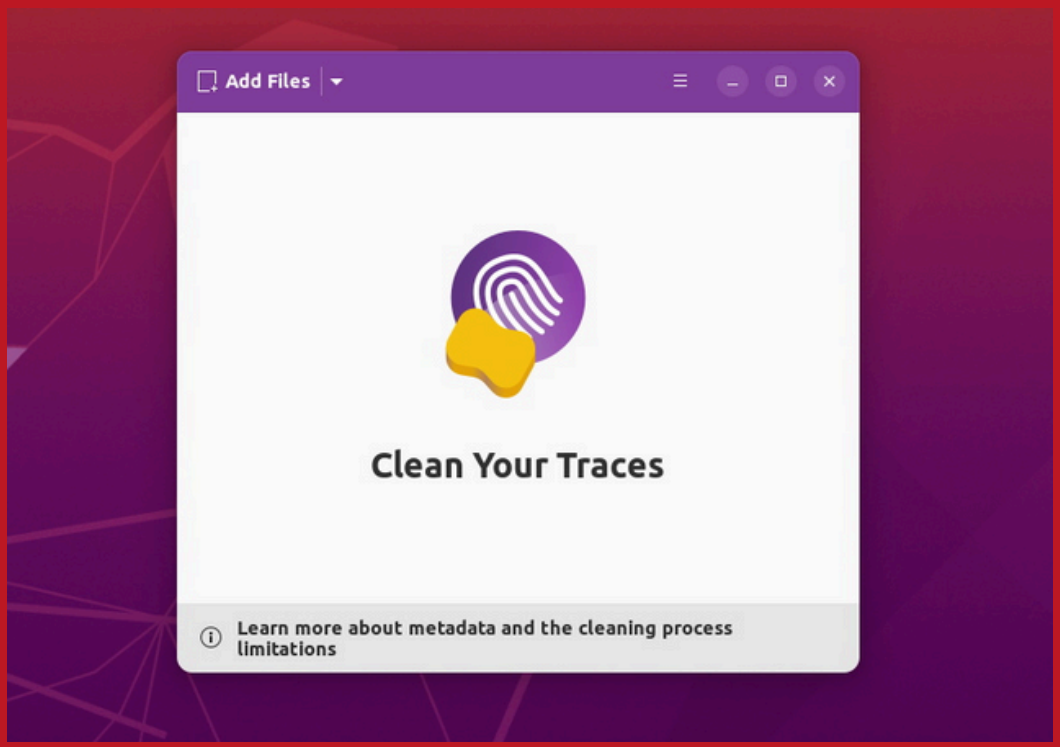


È stato sviluppato come progetto alternativo senza scopo di lucro. Grazie alla privacy e alla sicurezza che garantisce, rende sostanzialmente più difficile lo sfruttamento delle fonti di vulnerabilità più comuni. Migliora la sicurezza sia del sistema operativo che delle app in esecuzione su di esso.

GrapheneOS aggiunge varie impostazioni per funzionalità come l'autorizzazione di rete, l'autorizzazione dei sensori (microfono, fotocamera, ecc.), le restrizioni quando il dispositivo è bloccato (USB-C/pogo pin, fotocamera, ecc.) insieme a funzionalità di privacy e sicurezza più complesse rivolte all'utente. Si consiglia di installare GrapheneOS per un utilizzo sicuro dei telefoni.

Informazioni sull'Archiviazione

Ogni file (video, foto, pdf ecc.) contiene metadati, ovvero informazioni relative alla data di creazione, modifica, dimensione, fotocamera, formato, applicazione utilizzata per crearlo e modificarlo. Anche la geolocalizzazione è un metadata. Si tratta del processo di determinazione della posizione fisica di un dispositivo utilizzando tecnologie come GPS, Wi-Fi o reti cellulari. Fornisce informazioni sulla posizione di un dispositivo, spesso espresse in coordinate o in un indirizzo fisico. Si consiglia di controllare il proprio dispositivo per rendere difficile l'accesso al suo contenuto. Esiste il pericolo costante di diffondere i metadati tramite e-mail/SMS/social network dei file. È auspicabile rimuoverli, soprattutto in caso di pubblicazione su Internet o condivisione (tramite messaggio o e-mail). A questo scopo esiste l'applicazione Metadata Cleaner su Tails/Debian/Linux o, per il telefono, l'applicazione Image Pipe.



1. Come evitare la diffusione di informazioni su Internet?

Quando si utilizza Internet, molte informazioni circolano e vengono salvate per diversi anni. Queste variano a seconda del sito web che visitiamo, del telefono che utilizziamo, della rete Wi-Fi, della condivisione della connessione Internet, ecc. Esistono alcune soluzioni per ridurre lo spionaggio e l'identificazione durante la navigazione in Internet.

VPN

Il ruolo del VPN (Virtual Private Network) è quello di nascondere la posizione della tua connessione e garantire una maggiore protezione delle tue informazioni. Il VPN stabilisce una connessione sicura e affidabile sovrapponendosi a una rete non sicura, proteggendo la tua attività online, la tua posizione e la tua identità.

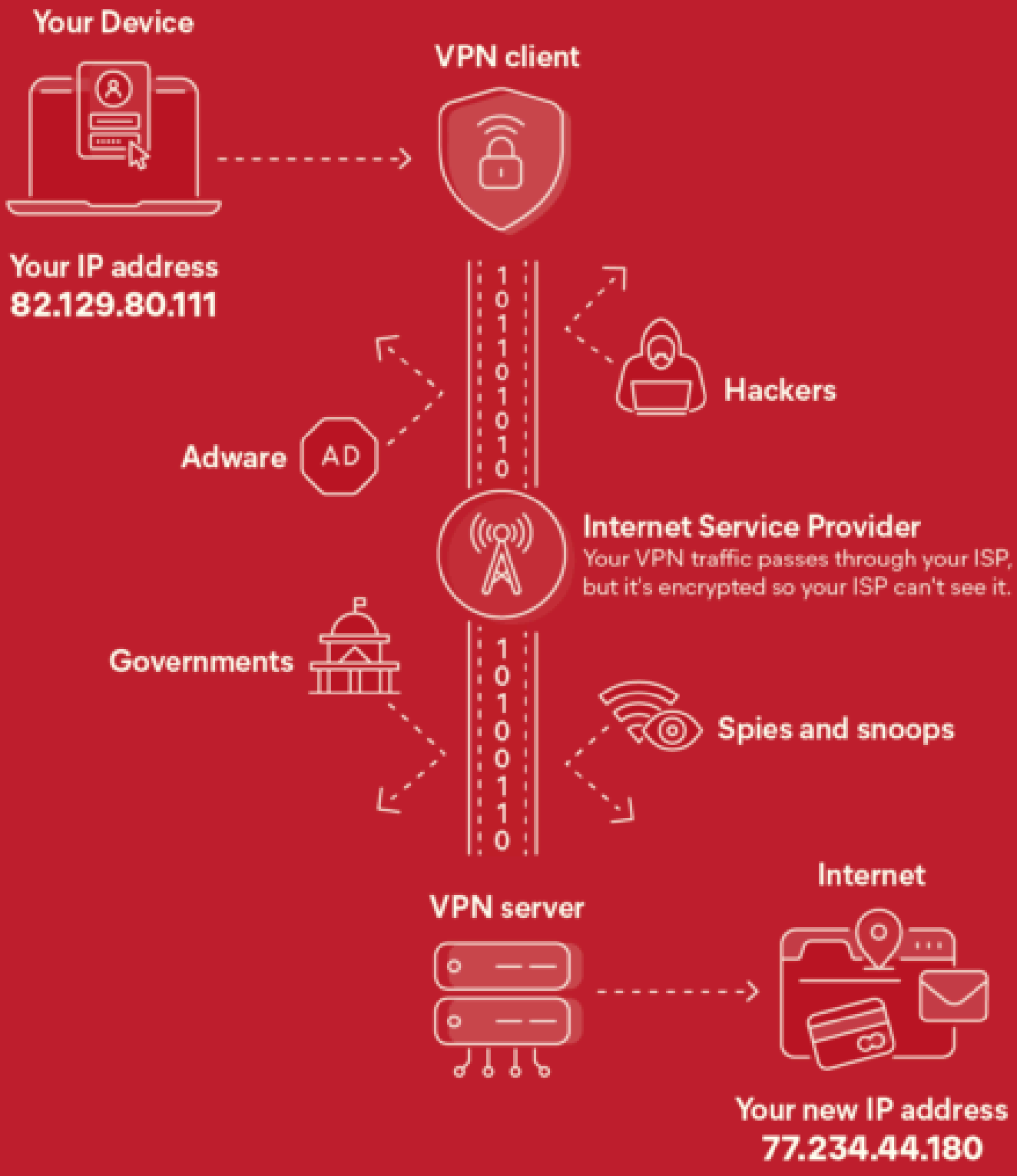
Come funziona?
Quando ti connetti a Internet, ogni connessione ha un indirizzo assegnato, ad esempio, se sei connesso a Internet da casa, questa connessione ha un indirizzo, un codice, chiunque si connetta sarà identificato come presente a quell'indirizzo. Questo indirizzo è chiamato indirizzo IP.

Questo è il pericolo: se il nemico conosce il tuo dispositivo e ti sta spiando, la tua posizione reale sarà facilmente identificabile quando ti connetti a una rete senza utilizzare un VPN, esponendo la tua posizione e rivelando che si tratta di un luogo di compagne/i.

La funzione del VPN è quella di modificare questo indirizzo e anche di nascondere le informazioni inviate, rendendo praticamente impossibile il lavoro del nemico. Il VPN inserirà le tue informazioni in una scatola protetta da una chiave: se il nemico tenterà di intercettare le tue informazioni tramite spionaggio digitale, non sarà in grado di aprire questa scatola.

Esistono alcuni provider VPN gratuiti e completamente anonimi, come RiseUp VPN, che può essere installato su qualsiasi dispositivo. RiseUp VPN non è compatibile con i dispositivi Apple iOS. Anche Proton Mail VPN funziona senza pagamento su iOS, ma richiede l'accesso alla posta elettronica su alcuni dispositivi. Altri provider sicuri, come Mullvad, PIA ecc., sono a pagamento, ma sono comunque validi e sicuri.

When you use a VPN



Tor Browser

Il browser TOR è la soluzione migliore per effettuare ricerche, guardare video o pubblicare contenuti su Internet in modo semplice e sicuro. Non registra la cronologia di navigazione né le password e consente di nascondere all'operatore Internet e ai siti web visitati l'identità dell'utente. Utilizza diversi punti di trasmissione che consentono di rendere anonime le nostre connessioni e il nostro lavoro. È disponibile su tutti i telefoni e computer.

https://www.torproject.org/

2. Da cosa proteggersi?

È difficile verificare se un componente di un telefono sia stato fisicamente modificato e/o danneggiato da nemici. Intorno a noi abbiamo migliaia di dispositivi elettronici come telefoni, computer, ecc. Inoltre, la maggior parte delle nostre comunicazioni passa attraverso gli stessi dispositivi. Ciò rende ancora più necessario utilizzarli in modo sicuro e consapevole per difendersi dalle minacce online. Le minacce online sono insiemi di pratiche e tecniche volte a invadere i dispositivi, spiare, raccogliere e alterare i dati. Per contrastare questo fenomeno, la sicurezza digitale consiste in tecniche e pratiche che rendono più sicuro l'uso della tecnologia.

Tipi di Attacchi

Malware

Il “malware” è qualsiasi tipo di software progettato per danneggiare un computer. Il malware può rubare informazioni sensibili dal tuo computer, rallentarlo gradualmente o persino inviare e-mail false dal tuo account di posta elettronica a tua insaputa.

Ecco alcuni tipi comuni di malware di cui potresti aver sentito parlare:

- **Virus:** un programma dannoso in grado di copiare se stesso e infettare un computer.
- **Worm:** un programma dannoso che invia copie di se stesso ad altri computer tramite una rete.
- **Spyware:** malware che raccoglie informazioni dagli utenti a loro insaputa.
- **Adware:** software che riproduce, visualizza o scarica automaticamente pubblicità su un computer.
- **Cavallo di Troia:** programma distruttivo che finge di essere un'applicazione utile, ma danneggia il computer o ruba informazioni dopo essere stato installato.

Come si diffonde il malware:

- Scaricando programmi da Internet che contengono segretamente dei malware
- Visitando un sito web infettato da malware
- Cliccando su un falso messaggio di errore o una finestra pop-up che avvia il download del malware
- Aprendo un allegato e-mail che contiene malware
- Tramite chiavette USB e dischi rigidi

Esistono molti modi diversi in cui il malware può diffondersi, ma ciò non significa che tu sia impotente nel fermarlo. Ora che sai cos'è il malware e cosa può fare, esaminiamo alcune misure pratiche che puoi adottare per proteggerti.

Come prevenire il malware:

- Mantieni aggiornati il computer e il software
- Non collegare chiavette USB che non sono affidabili
- Usa Linux → per una maggiore sicurezza, il malware di solito funziona solo su Windows
- Pensaci due volte prima di cliccare su link o scaricare qualsiasi cosa

Phishing

Utilizzato per rubare informazioni, inclusi login, accessi, dati. Eseguito principalmente tramite e-mail, messaggi e telefonate.

Come difendersi:

- Controlla se l'origine del messaggio e-mail è affidabile.
- Se contiene indirizzi web sospetti.
- Se possibile, verifica sempre l'affidabilità del messaggio con la persona che lo ha inviato.

“Attacco Man in the Middle”

Quando il nemico si connette alle nostre reti, può spiare le informazioni che un dispositivo invia tramite Internet. Questo attacco può essere effettuato tramite malware, attraverso una rete non sicura, da agenti sul campo e quindi ottenere informazioni sensibili.

Come proteggersi:

- Evitare connessioni WiFi non protette da password.
- Prestare attenzione alle notifiche del browser che segnalano un sito web come non sicuro.
- Disconnettersi immediatamente da un'applicazione sicura quando non è in uso.
- Non utilizzare reti pubbliche (ad esempio bar, hotel) quando si effettuano transazioni sensibili.
- Utilizzare TOR come browser Internet

3. Cyber War

Con lo sviluppo di tutte queste tecnologie, è diventato chiaro che gli Stati avrebbero utilizzato questi strumenti e queste tecniche per attaccare, spiare e raccogliere informazioni. Anche altri Stati come Stati Uniti, Russia, Ucraina, Israele e Iran stanno diventando sempre più professionali nell'effettuare attacchi. La NATO sta effettuando sempre più attacchi e addestramenti in questo settore.

Questo lo possiamo vedere molto bene nell'esempio del malware Stuxnet. S**tuxnet è un worm informatico** dannoso scoperto per la prima volta nel 2010 e che si ritiene fosse in fase di sviluppo almeno dal 2005. **Stuxnet prende di mira i sistemi di controllo su computer e software** e si ritiene che sia responsabile di aver causato danni sostanziali al programma nucleare iraniano. Sebbene né gli Stati Uniti né Israele abbiano ammesso apertamente la propria responsabilità, diverse testate giornalistiche indipendenti sostengono che Stuxnet sia un worm informatico creato dai due paesi in collaborazione. Stuxnet agisce prendendo di mira i computer che utilizzano il sistema operativo Windows e le reti. Ha cosi' individuato il software Siemens Step7 utilizzato nel programma nucleare. Secondo quanto riferito, Stuxnet ha compromesso i sistemi di controllo iraniani, raccogliendo informazioni sui sistemi industriali e causando la rottura delle centrifughe ad alta velocità. Stuxnet avrebbe distrutto quasi un quinto delle centrifughe nucleari iraniane. Prendendo di mira i sistemi di controllo industriale, il worm ha infettato oltre 200.000 computer e causato il deterioramento fisico di 1.000 macchine.

Questo non è poi così lontano dalla nostra realtà. **La Francia ha creato un malware per spiare file, informazioni e posizioni, soprattutto in Siria.** Ancora oggi vediamo questo virus infettare dispositivi e circolare nelle nostre istituzioni. Un buon esempio è il **malware Babar**, reso pubblico dall'informatore Edward Snowden. Lo spyware Babar è in grado di registrare i tasti digitati, i contenuti degli appunti, di acquisire schermate e persino di registrare conversazioni audio tramite Skype e Yahoo. Può iniettare codici nei processi in esecuzione e rubare file. Utilizza inoltre una rete Tor per comunicare in modo segreto. Questo spyware è sicuramente uno strumento di spionaggio e potrebbe essere stato utilizzato per vari motivi politici.

La Turchia, nonostante molte debolezze, ha in programma di diventare una potenza nel campo degli attacchi e dello spionaggio digitale. Per quanto riguarda lo spionaggio digitale, attualmente esiste una legge secondo cui, affinché Google, Meta (Facebook, Whatsapp, Instagram) possano operare sul loro territorio, queste aziende devono fornire tutti i dati richiesti, come la posizione, i messaggi, l'accesso alle foto, ecc., nonché quasi tutti gli account sulle piattaforme di media digitali da loro richiesti. Soprattutto prima degli attacchi e delle operazioni da parte dello Stato, i media digitali come Meta bloccano gli account che condividono contenuti politici come metodo di censura. **Ad esempio, prima dell'inizio degli attacchi dello Stato turco contro il Rojava, gli account sulle piattaforme di media digitali come Instagram, Twitter ecc. che potrebbero mobilitarsi contro questi attacchi vengono bloccati e chiusi.** Le capacità operative dei servizi di intelligence digitale sono utilizzate principalmente per la sorveglianza interna e lo spionaggio contro i loro avversari politici, utillizzando programmi di sorveglianza di potenze come

Israele. Inoltre, è già stato dimostrato che vengono spiati i servizi telefonici di altri paesi come Armenia, Grecia, Israele e Siria. L'organizzazione di intelligence dello Stato turco MIT afferma anche di lavorare sulla sicurezza digitale, sui satelliti e sull'intercettazione dei segnali in tutto il mondo.

In questa realtà, dobbiamo diventare consapevoli del nostro uso delle tecnologie, soprattutto con il nostro nemico che si sta specializzando, dobbiamo anche noi diventare professionisti, diventare consapevoli e prepararci per una guerra che è già diventata reale. **Questa guerra deve seguire i nostri principi della Guerra Popolare Rivoluzionaria,** poiché una persona non protetta, una persona che non sta attenta, potrebbe mettere in pericolo decine di compagne/i. Dobbiamo rendere questo argomento un tema comune per tutti noi e per l'intera società. **Dobbiamo lavorare tutti insieme per proteggere le nostre identità, le nostre posizioni, i nostri messaggi e le nostre informazioni.**

4. Sicurezza di Telecamere e Microfoni:

Se il nemico vuole approfittare di voi tramite la sorveglianza con telecamere e microfoni, deve hackerare il vostro dispositivo. Quasi tutti gli attacchi hacker sono causati da malware. **L'apertura di allegati e-mail sconosciuti, il download da fonti sconosciute e la visita di siti web inaffidabili sono le cause del 98% circa dei malware che finiscono sui nostri dispositivi.**

Una volta installato il malware, il vostro computer o telefono è completamente esposto agli hacker. È possibile prevenirlo semplicemente evitando il malware e assicurandosi che il software antivirus sia attivo e aggiornato. Ma una volta che il malware è installato sul tuo computer, il nemico è in grado di accedere al tuo microfono e alla tua fotocamera.

La maggior parte dei computer ha microfoni e fotocamere integrati. Lo stesso vale per i telefoni. Pertanto, si consiglia di coprire tutte le fotocamere dei tuoi dispositivi. **Poiché le fotocamere e i microfoni integrati** sono direttamente collegati a Internet, sono molto facili da hackerare. In questo caso, il nemico può facilmente assumere il controllo della fotocamera e accenderla o spegnerla a suo piacimento, nonché disattivare la luce LED per evitare di essere rilevato. Naturalmente è possibile bloccare tutte le autorizzazioni e l'accesso al microfono e alla fotocamera. Nella maggior parte dei casi, la protezione software è più comoda di quella fisica, ma non sempre altrettanto affidabile. Esistono numerosi software che consentono di accedere a questa funzione. In particolare, GrapheneOS offre questa opzione per il dispositivo fin dall'inizio, oltre alla possibilità di verificare in qualsiasi momento se l'accesso al microfono e alla fotocamera è consentito o meno.

Anche se coprire la fotocamera con del nastro adesivo non impedisce a qualcuno di ascoltare attraverso il microfono, è comunque una buona protezione per il tuo anonimato. Certo, impedirà la videosorveglianza, ma il suono dal microfono potrà comunque essere registrato.

I laptop moderni hanno spesso diversi microfoni per migliorare la qualità del suono, e coprirli tutti con del nastro adesivo sarà difficile. In alcuni modelli, i microfoni integrati vengono disattivati quando si collega uno esterno.

Un trucco utile per loro è quello di collegare un adattatore al jack del microfono (o al jack universale per microfoni e cuffie). Il vostro laptop penserà che sia collegato un microfono esterno e disattiverà tutti quelli integrati.

Perché nella maggior parte dei casi, la protezione software è più comoda di quella fisica, ma non sempre altrettanto affidabile. Dobbiamo sempre stare attenti quando parliamo a non rivelare alcuna informazione al nemico mentre siamo vicini ai nostri dispositivi.

5. Come comunicare in modo sicuro

l'Applicazione Signal

Per comunicare in modo sicuro, è bene sapere se l'azienda che sviluppa l'applicazione del servizio di messaggistica collabora con la polizia, gli Stati, se vende dati ecc. o meno. Esistono diverse applicazioni che non sono sicure, come Whatsapp, ma alcune applicazioni per la comunicazione forniscono la crittografia. Naturalmente, con il tempo verranno sviluppate applicazioni migliori, ma c'è sempre la possibilità che le applicazioni utilizzate vengano prese in consegna dal nemico. Pertanto, in generale si raccomanda di prestare attenzione in materia di comunicazione su qualsiasi dispositivo per non esporre informazioni su queste piattaforme e applicazioni.

Per comunicare tramite messaggi/chiamate, l'applicazione SIGNAL offre un livello di crittografia molto elevato contro gli hacker. È disponibile su tutti i telefoni e anche sui computer. È possibile configurare messaggi effimeri e diverse opzioni per una maggiore sicurezza.

Come abbiamo detto in precedenza, **l'uso di applicazioni come Whatsapp non è sicuro: oltre a fornire informazioni allo Stato turco, Whatsapp ha una sicurezza molto debole contro gli attacchi** ed è molto facile scoprire informazioni attraverso tecnologie di spionaggio.

Un altro aspetto molto pericoloso di Whatsapp è che tutti i messaggi, anche quelli cancellati, vengono memorizzati nei file di Whatsapp. Se lo Stato turco richiede i vostri messaggi, i vostri affitti, le informazioni sul vostro numero, tutte le vostre informazioni verranno trasmesse. In questo caso, nemmeno l'uso di un VPN sarebbe una soluzione completa, poiché solo le vostre informazioni sarebbero protette, ma tutti i messaggi e le immagini continuerebbero ad essere condivisi anche diversi mesi dopo l'invio.

Tails

Inoltre, TAILS offre numerose opzioni per la comunicazione crittografata. In questo modo, gran parte della comunicazione può essere effettuata tramite i servizi disponibili su TAILS. Ciò può migliorare la nostra privacy online.

Tails include:

- Tor Browser con uBlock, un browser sicuro e un ad-blocker
- Thunderbird, per e-mail crittografate
- KeePassXC, per creare e memorizzare password complesse
- OnionShare, per condividere file, siti web e chat room su Tor
- Metadata Cleaner, per rimuovere i metadati dai file

6. Buone Pratiche

- **Utilizzare password diverse a seconda degli account e delle applicazioni.** La forza di una password è data dalla sua lunghezza, si parla addirittura di pass-sentence per una maggiore sicurezza. L'uso di caratteri speciali non migliora più la sicurezza di un identificatore. Si consiglia di creare una password composta da diverse parole casuali per un identificatore o un computer e una password di 12 caratteri per un telefono.

- **Utilizza applicazioni sicure consigliate dai compagni**. Installa app da fonti affidabili. Tails App sono sottoposte a controlli di sicurezza, riducendo il rischio di attività dannose relative al microfono o ad altre funzioni sensibili.

- **Non rispondere a messaggi provenienti da contatti sconosciuti o strani** e non aprire link che potrebbero essere stati inviati da questi, poiché il loro scopo è quello di ottenere la tua posizione.

- Mantieni la posizione (GPS) disattivata, la pratica migliore è quella di lasciare il cellulare sempre in modalità aereo. La modalità aereo può essere attivata mentre la connessione Wi-Fi è attiva.

- macOS:

- Non viaggiare con il cellulare acceso, se possibile rimuovi la scheda SIM prima di recarti in altri luoghi, questo impedisce anche che la tua posizione venga decifrata via satellite.

- **Acquista una custodia di sicurezza che blocchi il segnale (come una Faraday Bag).** Questo impedisce che qualsiasi segnale venga inviato dal tuo cellulare, rendendola la scelta migliore per i viaggi e i trasporti.

- **Non inviare messaggi con il tuo nome, la tua posizione, dove ti trovi e dove stai andando.** I messaggi, specialmente su Whatsapp, possono essere intercettati e utilizzati dai servizi segreti nemici.

- **Utilizza una soluzione antivirus/antimalware.** Si tratta di un software o servizio essenziale che protegge i sistemi informatici dai software dannosi. Questi programmi lo fanno rilevando possibili minacce malware, bloccandole prima che accedano al sistema ed eliminando quelle esistenti in modo che non causino ulteriori danni al sistema. A tal fine, esistono diversi software che puoi scaricare sui tuoi dispositivi. Questo vale per tutti i tipi di dispositivi come computer, telefoni di ogni sistema operativo e persino telefoni con GrapheneOS.

- **Mantieni aggiornato il tuo dispositivo.** Assicurati che il tuo dispositivo utilizzi l'ultima versione disponibile del sistema operativo e delle patch di sicurezza. Gli aggiornamenti regolari spesso includono correzioni di bug e miglioramenti della sicurezza che risolvono potenziali vulnerabilità. Non aggiornare per garantire la sicurezza è un pensiero comune o una falsa convinzione. È meglio aggiornare per garantire la sicurezza di un dispositivo che ha accesso a Internet.

Conclusione

Con questo piccolo protocollo di sicurezza digitale abbiamo voluto condividere con voi alcune informazioni di base su come proteggervi a livello digitale. Poiché gli attacchi informatici sono in aumento e l'uso delle comunicazioni digitali e delle piattaforme diventa sempre più presente, è importante per noi sapere come utilizzarle in modo sicuro e come proteggerci o prevenire eventuali attacchi da parte dello Stato o di altri nemici. Poiché siamo la parte anticapitalista della società che combatte contro questo sistema, dobbiamo sempre ricordare a noi stessi che possiamo diventare bersagli di tali attacchi. Pertanto, prendere sul serio la nostra sicurezza è una questione molto importante ed essenziale per tutti noi nella vita quotidiana.

internationalistcommune.com