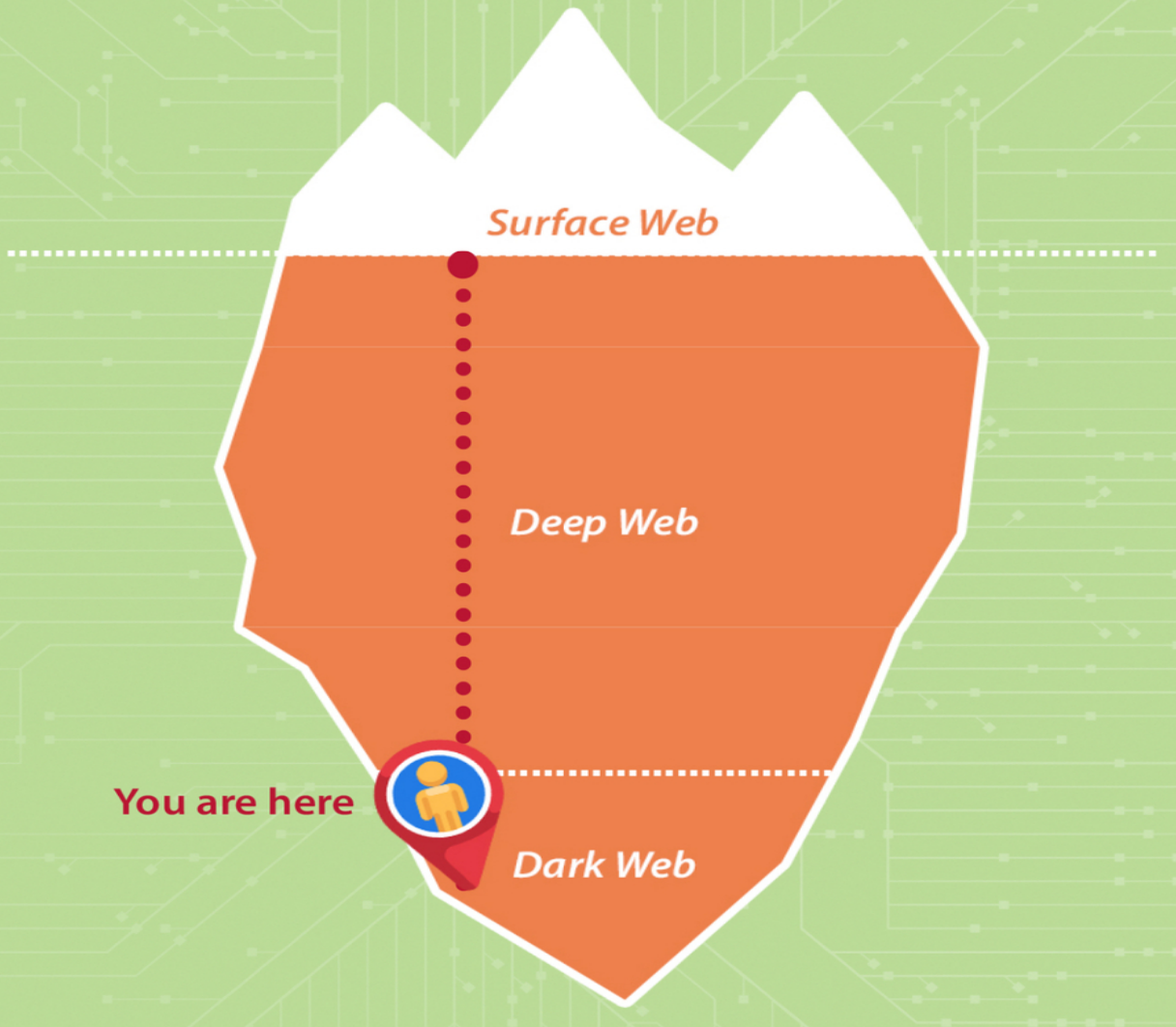
DANILO CIMINO

DEEP WEB E DARK WEB

GUIDA COMPLETA ALL' ANONIMATO SU INTERNET



Cosa sono Deep Web e Dark Web, come entrare, come acquistare merce, come navigare in modo sicuro ed anonimo su internet

SOMMARIO

DEEP WEB E DARK WEB

GUIDA SEMPLICE ALL'ANONIMATO ONLINE E ALLA NAVIGAZIONE SICURA

Cosa sono deep web e dark web, come entrare, come acquistare merce, come navigare in modo sicuro ed anonimo su internet

INTRODUZIONE

"Ma che è sto dark web?"

"Ma dark web e deep web sono la stessa cosa"

"Non esiste anonimato su internet"

"TOR non è altro che due VPN a cascata"

"Non ho mai capito come si accede al deep web"

"Basta una VPN e sei anonimo"

"Cosa trovi sul dark web?"

"Io uso sempre la modalità incognito e sono a posto"

Quelli che hai appena letto sono commenti veri di persone che mi seguono sui social. Il deep web ed il dark web sono argomenti che suscitano molta curiosità ma anche moltissima confusione.

A proposito: mi chiamo Danilo e riesco a spiegare l'informatica in modo chiaro e comprensibile. E non sono io a dirlo: lo dicono tutti quelli che si prendono la briga di lasciarmi delle testimonianze o di scrivermi in privato per ringraziarmi.

Faccio il consulente informatico, il content creator (creatore di contenuti) ed il divulgatore. Gestisco il progetto "cose di computer", dedicato principalmente alle persone "poco tecnologiche". Il mio scopo è migliorare la vita digitale di chi mi segue.

Come? Offrendo quasi ogni giorno dei contenuti che riguardano l'informatica. Tutto quello che spiego è fatto apposta per essere compreso da chiunque: niente paroloni, niente sigle strane, niente uso eccessivo della lingua inglese.

Ogni volta che parlo di deep web, dark web e privacy su internet, immancabilmente qualcuno mi fa delle domande. Rispondo sempre a tutti ma il problema è che l'argomento è sconfinato, è difficile dare una risposta chiara e precisa in un video di pochi secondi o in un testo leggibile in soli due minuti.

Ho deciso allora di scrivere questo manuale, per darti la possibilità di capire DAVVERO cosa voglia dire il termine "privacy" quando si parla di internet.

Per navigare in modo sicuro ed anonimo non basta seguire una procedura prestabilita o usare un determinato programma, come fai normalmente quando navighi in rete. Devi conoscere (anche solo sommariamente) alcuni concetti informatici fondamentali. Lo scopo di questo manuale è farti capire bene questi concetti.

COSA TROVERAI IN QUESTO MANUALE

Le pagine che stai per leggere contengono tutto quello che ti serve per navigare in modo sicuro ed anonimo su internet (per quanto possibile). Ti spiegherò in modo molto elementare ciò che non puoi fare a meno di conoscere per mascherare il più possibile la tua identità quando sei in rete.

"Ma non è illegale?". No: essere anonimi non vuol dire essere dei criminali (o almeno non necessariamente). Questo manuale non è rivolto ai delinquenti ma a tutti coloro che, per un motivo o per un altro, hanno la necessità di non far sapere a nessuno quello che fanno su internet.

Pensa ad esempio ad un giornalista di un paese non democratico, che ha la necessità di aggirare la censura imposta dal governo. Oppure ad una persona che vuole comunicare informazioni "scottanti" senza subire ritorsioni.

Gli strumenti per la tutela della privacy sono sempre esistiti, nel bene e nel male. Io ti spiegherò quali sono quelli che abbiamo a disposizione quando andiamo in rete.

COSA NON TROVERAI IN QUESTO MANUALE

Te lo dico subito: se sei un esperto di informatica, questo libro potrebbe non piacerti. Potrebbe addirittura farti arrabbiare, al punto da indurti a contattarmi per correggermi o per mandarmi a quel paese.

Io sono un divulgatore ed ho la necessità di farmi capire da tutti. Pertanto quando spiego le cose devo sacrificare gli aspetti più tecnici per dare priorità alla comprensibilità.

Ecco un paio di definizioni che generano sempre commenti schifati:

Un indirizzo IP è composto da 4 numeri separati da dei puntini.

Un server è un computer sempre acceso e sempre collegato ad internet.

Guarda ora una definizione di Wikipedia:

Un indirizzo IP (dall'inglese Internet Protocol address) è un numero del pacchetto IP che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete per l'instradamento/indirizzamento, inserito dunque nell'intestazione (header) del datagramma IP per l'indirizzamento tramite appunto il protocollo IP.

Il 99% delle persone non sono in grado di capire questa definizione. Non pretendo di essere "superiore" a Wikipedia (non è questo il punto). È solo che le mie definizioni non ambiscono ad essere dettagliate dal punto di vista scientifico ma ad essere comprensibili da chiunque.

Non ti piace quello che faccio? Pazienza, sono consapevole di non poter piacere a tutti. Sono anche consapevole del fatto che molte persone, grazie ai miei contenuti, riescono finalmente a "capirci qualcosa".

DISCLAIMER (DICHIARAZIONE DI ESCLUSIONE DI RESPONSABILITÀ)

Questo manuale è stato redatto a scopo esclusivamente informativo. Le informazioni che trovi qui sono di pubblico dominio. Io mi sto limitando ad esporre in modo chiaro e semplice concetti ben noti.

Io ti spiego delle tecnologie. L'uso che ne fai è una responsabilità esclusivamente tua. Ti invito caldamente a non usare le informazioni contenute in questo libro per compiere azioni illegali, anche perché se fai qualcosa di molto grave corri il rischio di essere rintracciato, a prescindere dalle contromisure che adotterai.

HO MOLTO DI PIÙ DA OFFRIRTI!

Visita il mio sito:

www.cosedicomputer.com

Iscriviti per ricevere GRATIS, direttamente nella tua casella email, i miei contenuti. Puoi anche seguirmi sul tuo social network preferito: pubblico di frequente dei brevi video che parlano di informatica ed internet.

COSA SONO LA PRIVACY E L'ANONIMATO?

La privacy è il diritto di tenere nascoste alcune informazioni che ci riguardano. Ed anche di controllare che tali informazioni vengano usate solo in caso di necessità.

Ad esempio: se un uomo soffre di una disfunzione erettile, ha il diritto di non farlo sapere a nessuno. Ed anche il diritto di rivelare questa informazione solo ed esclusivamente al suo medico curante (che dovrà comunque mantenere il segreto).

L'anonimato è invece una condizione: si è anonimi quando l'identità di una persona che compie una determinata azione non può essere accertata.

Ad esempio: marito e moglie usano lo stesso PC. Lui vuole acquistare a lei un regalo su internet senza farglielo sapere. Può farlo usando una scheda di navigazione in incognito (vedremo più avanti cos'è): in tal modo, lei non sarà in grado di vedere che lui ha visitato il sito sul quale ha comprato il regalo.

A meno di vivere in un paese non democratico, chiunque possiede il diritto alla privacy. Pertanto l'uso di strumenti di anonimizzazione è perfettamente legale.

Di questi tempi, visto che tutti usano sempre più di frequente PC e cellulari, siamo continuamente tracciati, monitorati e spiati in modi che probabilmente nemmeno ti immagini.

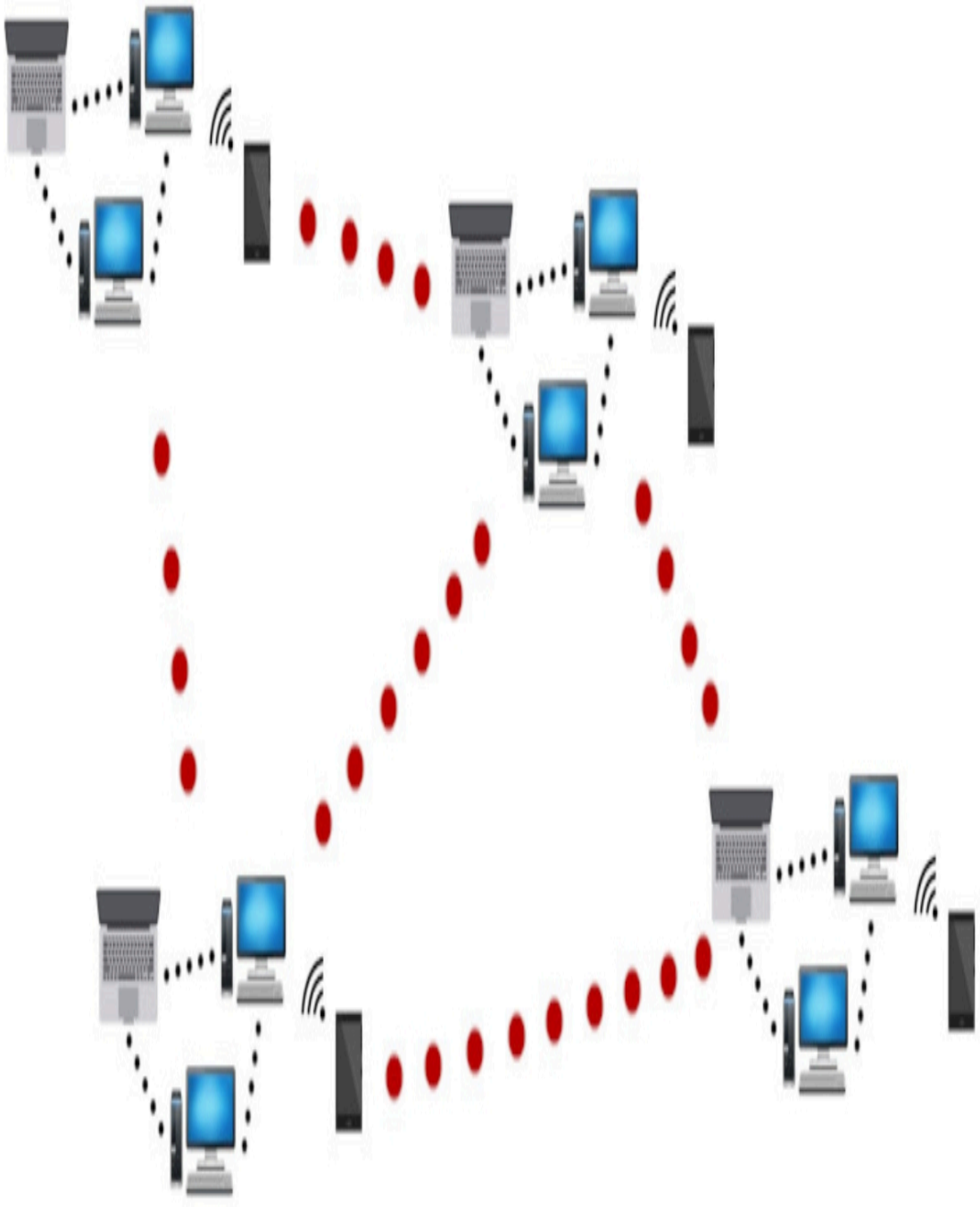
Nei prossimi capitoli troverai:

- Alcuni argomenti tecnici fondamentali
- Quali sono le forme di tracciamento a cui siamo sottoposti e come fare a neutralizzarle
- Una parte pratica in cui ti spiegherò come fare a navigare in modo anonimo e sicuro
- Un'altra parte pratica in cui spiegherò come accedere al dark web, come comprare merce e come cercare informazioni

Iniziamo coi concetti tecnici fondamentali.

COS'È INTERNET?

Internet è una rete di computer, o meglio una “rete di reti” in quanto collega tra loro sia singoli computer che intere reti locali, ad esempio reti aziendali o domestiche.



Lo scopo di internet è consentire la comunicazione a distanza fra i computer.

COS'È UN INDIRIZZO IP?

Esistono moltissimi tipi di computer in commercio: cellulari, tablet, PC ... (si: un cellulare moderno non è altro che un computer in miniatura!). Ognuno di essi funziona in modo diverso ed usa sistemi operativi diversi (Windows, Linux, macOS, iOS, Android eccetera).

È impossibile pretendere che tutti questi dispositivi si "capiscano" correttamente quando comunicano tra di loro. Pertanto, è necessario che parlino una “lingua comune”. Questa lingua comune si chiama "protocollo".

Internet è basata sul protocollo TCP/IP. TCP è una sigla che vuol dire “Transmission Control Protocol” (protocollo di controllo della trasmissione). IP è una sigla che vuol dire “Internet Protocol” (protocollo Internet). Non importa sapere esattamente come funziona TCP: quello che ci interessa di più è il protocollo IP.

Per spiegartelo in modo semplice userò un’analogia. Come ben sai, chiunque può spedire una lettera cartacea all’altro capo del mondo. Ti basta infilare un foglio in una busta, scrivere un indirizzo e depositare la missiva in una cassetta postale. Qualcuno la trasporterà all’indirizzo che hai scritto. Internet funziona allo stesso modo: per poter raggiungere un altro computer della rete è necessario che esso abbia un indirizzo.

I computer però non comprendono il linguaggio naturale degli esseri umani: funzionano grazie alla matematica, quindi comprendono solo numeri. Pertanto l’indirizzo di un computer deve per forza essere espresso come un numero. Un indirizzo IP è composto da 4 numeri separati da dei puntini.


134.34.53.112
212.118.92.98
221.45.6.19
121.234.12.37

Quando ti colleghi ad internet, il tuo "provider" (l'azienda che ti fornisce la connessione) ti assegna uno di questi indirizzi IP, che è un dato estremamente sensibile (vedremo più avanti perché).

COS'È IL WEB?

Internet è una rete che fornisce "servizi". Sono funzionalità che non avrebbero senso di esistere senza una rete sottostante. Tra i molti servizi offerti da internet troviamo:

- L’email (posta elettronica): è l’equivalente elettronico della posta tradizionale cartacea. Consente di inviare e ricevere messaggi via internet

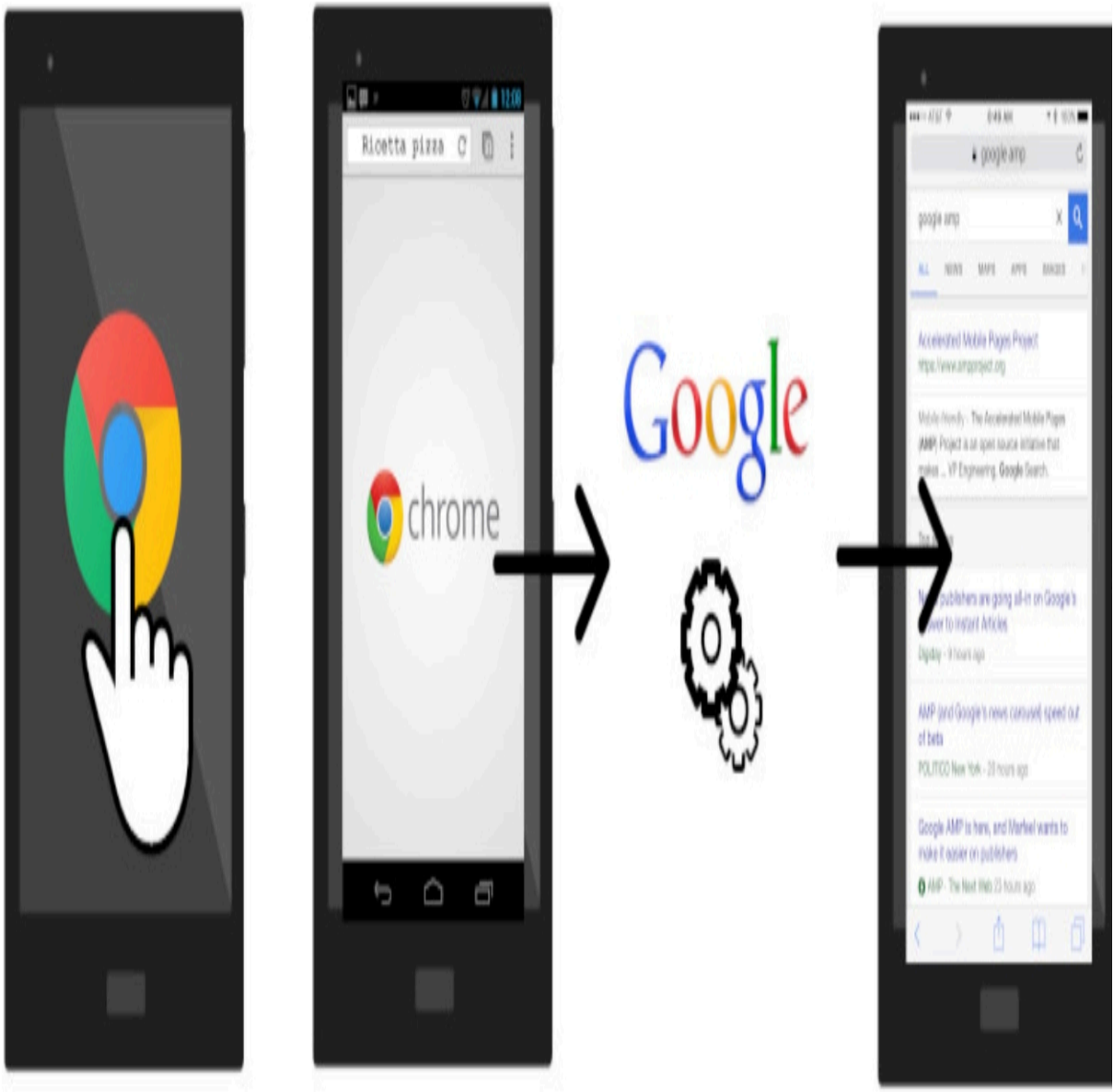
- WhatsApp: è un servizio di "messaggistica istantanea". Consente di inviare messaggi in modo immediato. In realtà anche le email vengono consegnate praticamente subito, però i messaggi WhatsApp sono stati pensati per essere letti appena arrivano, a differenza delle email

- Google: è un servizio di ricerca di informazioni

- Facebook: è un servizio di “social networking” (rete sociale) che aiuta le persone a restare in contatto tra loro

- Il web: è un servizio di consultazione di testi in rete. Un sito web è un contenitore di pagine che possiedono dei collegamenti tra loro, chiamati “link”. Per usare il servizio web, devi lanciare un programma dedicato chiamato “browser web“. Google Chrome, Edge, Safari e Firefox sono tutti esempi di browser web

  Il browser non è il motore di ricerca! Quando tiri fuori il cellulare dalla tasca e digiti, ad esempio, "ricetta pizza" nella barra del browser, in realtà stai dando queste parole in pasto a Google.

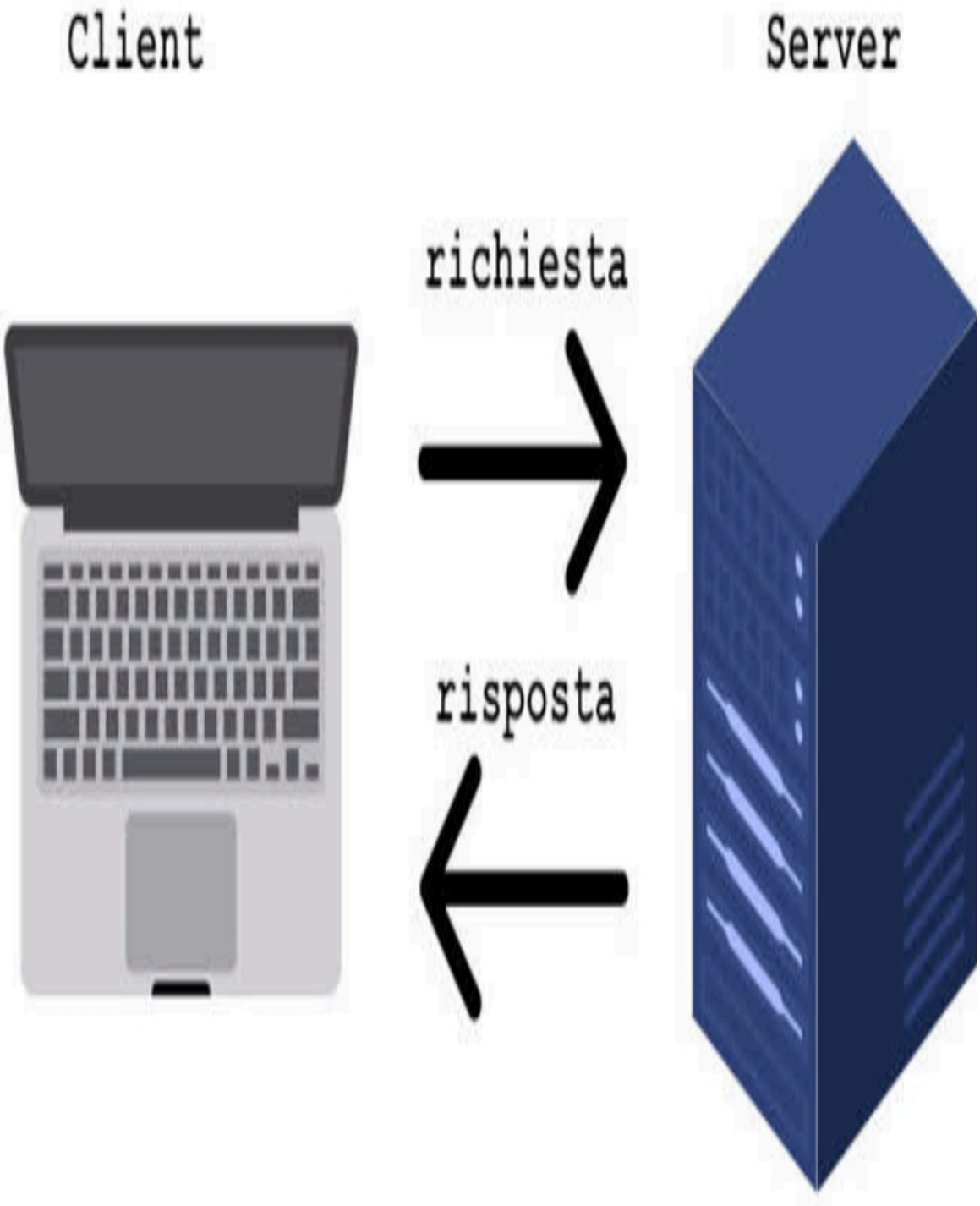

Ricetta pizza
chrome
Google
google amp
Accelerated Mobile Pages Project

Google ti restituirà una pagina con una lista di siti rilevanti per le parole che hai digitato.

COSA SONO I SERVER?

La maggior parte dei servizi internet funziona seguendo il "modello client-server". Te lo spiego con un esempio: vuoi consultare il tuo sito preferito di notizie. Quello che probabilmente fai di solito è prendere il cellulare, aprire il tuo browser preferito (tipicamente Google Chrome) e scrivere, ad esempio, “il Fatto Quotidiano”. Poi premi sopra al link che ti esce fuori fra i primi risultati ed inizi a leggere le notizie.

Quello che è successo è che il tuo cellulare (il “client”, “cliente”) ha mandato via internet una richiesta ad un altro computer chiamato “server“ (“servitore”), che ospita le pagine web contenenti gli articoli del Fatto Quotidiano.


Client
Server
richiesta
risposta

I server pertanto sono computer che rispondono alle richieste di altri computer, allo scopo di erogare un servizio.

Non c’è alcuna differenza tecnica tra un server ed un altro computer qualunque. Puoi pensare ad un server come ad un computer sempre acceso, sempre collegato ad internet, molto potente (quindi con tanta RAM e tanti Gigahertz) e pensato apposta per gestire un carico elevato di richieste.

COSA VUOL DIRE ESSERE ANONIMI SU INTERNET?

Anche se non te ne accorgi, quando usi un servizio internet vieni continuamente tracciato, monitorato, controllato e registrato in modi che forse non potresti nemmeno lontanamente sospettare. Giusto per dartene un’idea, riprendiamo l’esempio del servizio web. Tiri fuori dalla tasca il telefono e cerchi su Google il sito del Fatto Quotidiano. Ecco una lista approssimativa di quello che succede:

- Il tuo cellulare (o meglio: il tuo sistema operativo) memorizza da qualche parte il fatto che tu hai avviato un browser web ad un determinato giorno ed orario

- Il tuo browser web memorizza il giorno e l’ora esatta in cui hai visitato il sito del Fatto Quotidiano

- Se usi Chrome, Google (l'azienda che ti offre gratuitamente il browser Chrome) memorizza il giorno e l’ora esatta della visita

- Il tuo provider (l'azienda che ti fornisce la connessione: Vodafone, TIM ...) memorizza anche lui giorno ed ora esatta della visita

- Il server in cui è ospitato il sito web del Fatto Quotidiano memorizza il tuo indirizzo IP, insieme al giorno ed all'orario esatto della visita

Per la maggior parte delle persone questo non rappresenta un problema. Che succede però se si ha la necessità di non lasciare alcuna traccia?

E non sto parlando di un malintenzionato: pensa di nuovo al giornalista del paese non democratico, che deve comunicare qualcosa cercando di aggirare la censura imposta dal suo governo. Come può fare?

Non ha altra scelta se non annullare una per una queste forme di tracciamento. Nei prossimi capitoli vedremo come fare.

EVITARE IL TRACCIAMENTO DEL SISTEMA OPERATIVO

Come detto, il sistema operativo memorizza in modo molto accurato tutta la tua attività, sotto forma di "eventi" messi dentro ai cosiddetti "file di log".

È praticamente impossibile impedire che lo faccia. È anche molto difficile cancellare i file di log dopo che sono stati scritti, perché i file non vengono mai davvero "cancellati". Non basta svuotare il cestino: in moltissimi casi è possibile recuperare i file anche dopo che il cestino è stato svuotato.

L'unica soluzione possibile è utilizzare un sistema operativo "amnesico", ovvero pensato apposta per non ricordare nulla di quello che fai. Funziona così:

- Lo scarichi
- Lo installi su una chiavetta USB
- Inserisci la chiavetta dentro al tuo PC
- Fai partire il PC dalla chiavetta USB

Ed è fatta: nel momento in cui stacchi la chiavetta o spegni il computer, nulla di quello che hai fatto verrà ricordato.

Più avanti ti spiegherò dettagliatamente come preparare la tua chiavetta USB per la navigazione amnesica.

EVITARE IL TRACCIAMENTO DEL BROWSER

Per evitare il tracciamento dei browser, ovvero per fare in modo che esso non ricordi le pagine che hai visitato, devi usare le finestre anonime. Per attivarne una su Google Chrome, devi premere sul menu in alto a destra (quello coi tre puntini verticali) e selezionare “nuova scheda di navigazione in incognito”.


Stai navigando in incognito
Ora puoi navigare in privato. Le altre persone che usano questo dispositivo non vedranno le tue attività, ma i download, i preferiti e gli elementi dell'elenco di lettura verranno salvati. Scopri di più
Chrome non salverà le seguenti informazioni:
• Cronologia di navigazione
• Cookie e dati dei siti
• Informazioni inserite nei moduli
La tua attività potrebbe comunque essere visibile:
• Ai siti web visitati
• Al tuo datore di lavoro o alla tua scuola
• Al tuo provider di servizi Internet
Blocca cookie di terze parti
Se questa opzione è attiva, i siti non possono utilizzare i cookie per monitorare la tua attività sul Web. Le funzionalità su alcuni siti potrebbero non essere disponibili.

Attenzione: anche se si chiama “in incognito”, questa modalità NON GARANTISCE ASSOLUTAMENTE L'ANONIMATO! Evita solo che il browser inserisca le pagine che visiti all’interno della “cronologia” (ovvero l’elenco dei siti visitati). Evita anche parzialmente il tracciamento di alcuni siti ma in modo poco efficace. Questa modalità è da usare se:

- Vuoi leggere la tua posta elettronica da un PC pubblico o da casa di un amico

- Vuoi visitare un sito per adulti

- Vuoi acquistare un regalo ad un familiare che ha accesso allo stesso PC che stai utilizzando tu

- ... in ogni altro caso in cui non vuoi che, digitando qualcosa sulla barra del browser, venga fuori come suggerimento qualcosa di imbarazzante o riservato

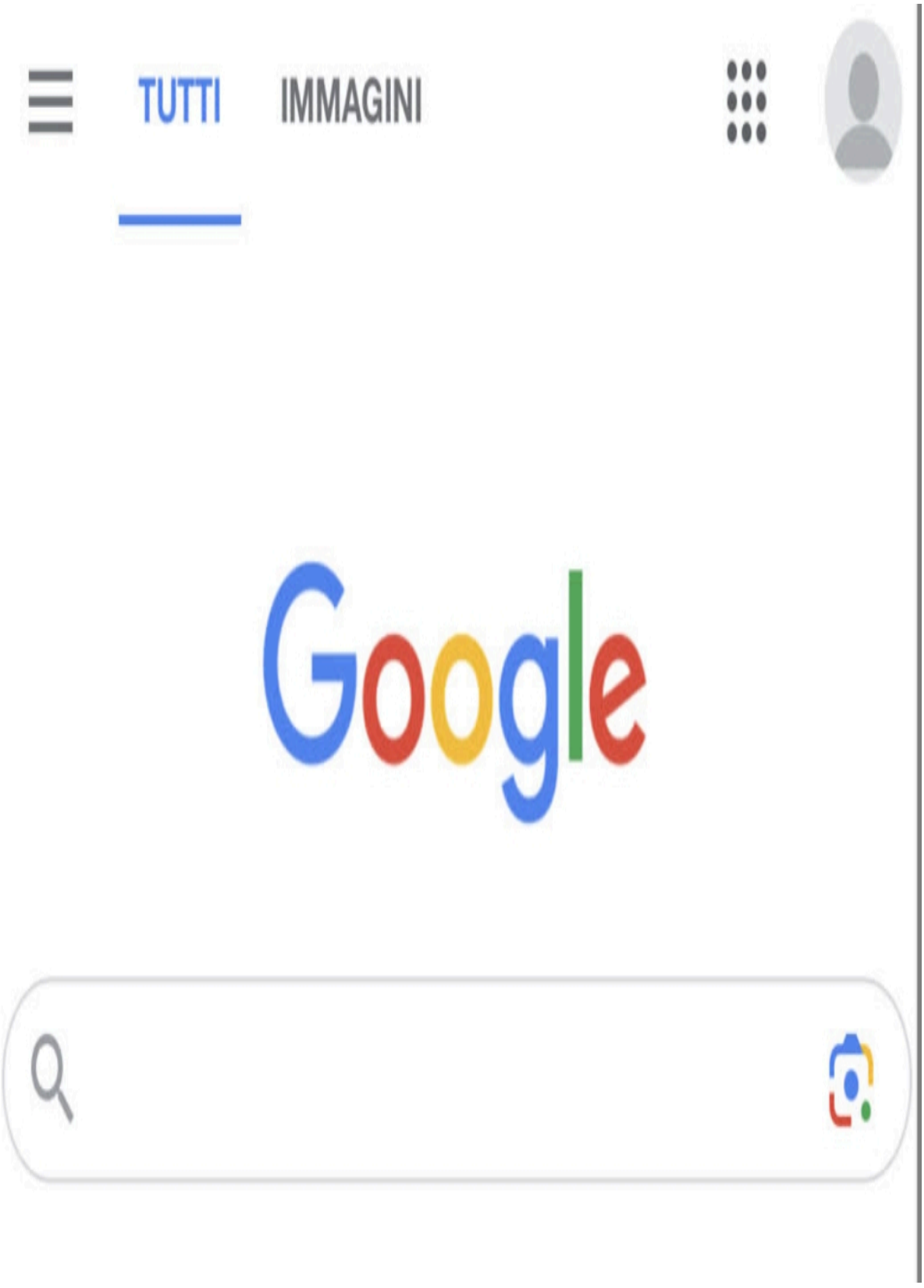
EVITARE IL TRACCIAMENTO DI GOOGLE

Anche se forse non lo sai, quasi sicuramente hai un account Google. E quasi sicuramente lo confondi col tuo indirizzo Gmail. Solo che sono due cose diverse: Gmail è un servizio di posta elettronica mentre un account Google è un contenitore di informazioni che ti riguardano.

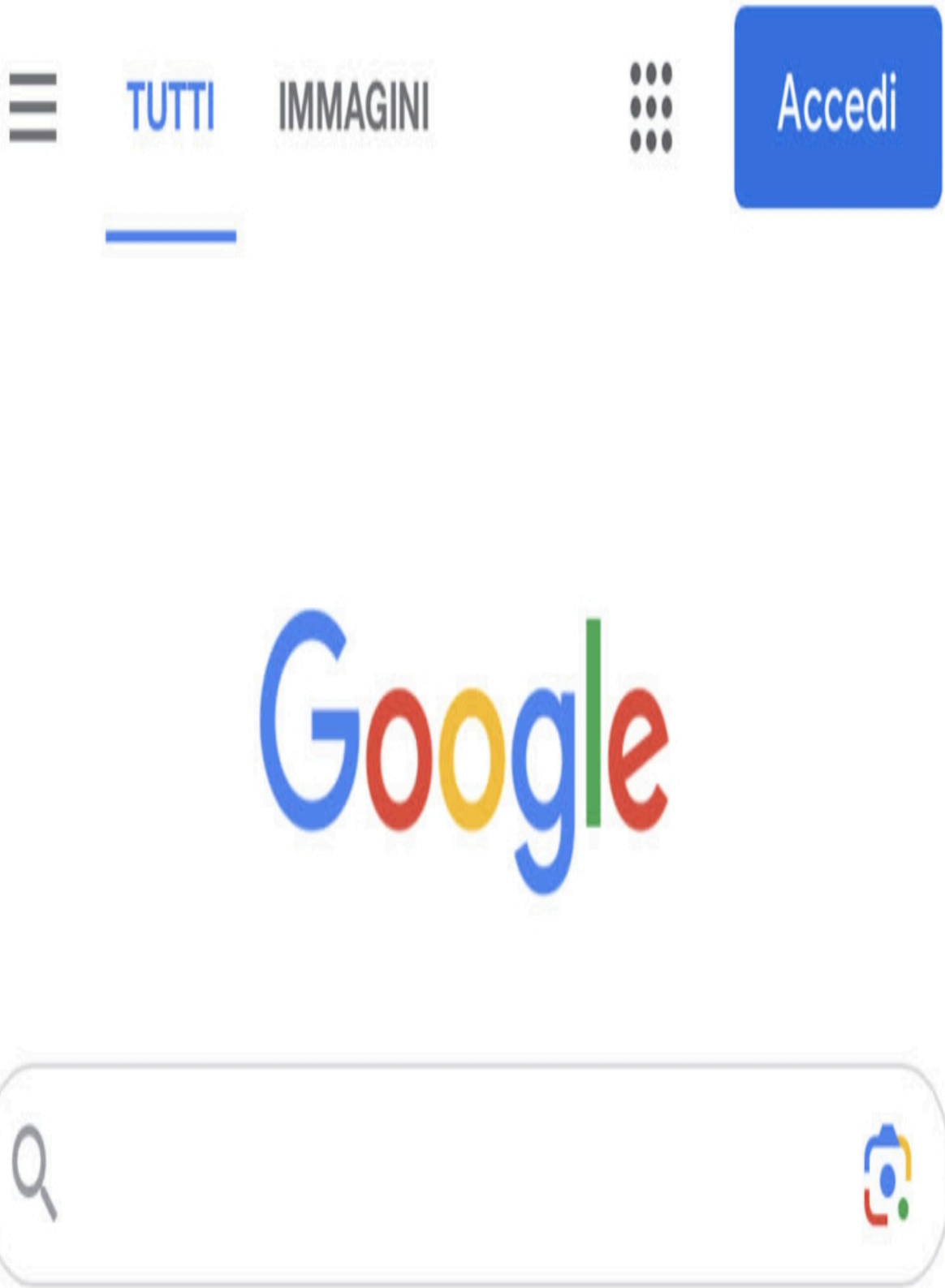
Perché Google raccoglie tutti questi dati? Semplice: guadagna miliardi di dollari dalla vendita di spazi pubblicitari. Deve garantire ai suoi inserzionisti di mostrare a chi naviga su internet le pubblicità che siano attinenti ai loro interessi. Pertanto, Google cerca di capire che tipo di persona sei.

Questa operazione si chiama “profilazione”. Se cerchi spesso ricette di dolci, Google se lo ricorderà. Ed ogni volta che visiterai un sito che usa il loro sistema pubblicitario (ovvero praticamente tutti), ti compariranno annunci di frullatori, tortiere ed altri prodotti simili.

Per evitare che accada, devi innanzitutto evitare di usare Google Chrome. Potresti ad esempio optare per Mozilla Firefox, un browser orientato alla privacy. Bada poi anche di non essere "loggato" (colelgato) al tuo account Google: apri una scheda del browser, vai su google.com e guarda nell’angolo in alto a destra. Se vedi una tua foto o un cerchietto con un omino dentro, premici sopra.


TUTTI
IMMAGINI
Google

Premi poi su “ESCI”, in basso. Dopo averlo fatto, in alto a destra, al posto del cerchietto, comparirà un tasto blu con scritto sopra “Accedi”. Da questo momento in poi non sarai più collegato al tuo account Google.


TUTTI
IMMAGINI
Accedi
Google

Questa operazione non evita completamente il tracciamento di Google. In molti casi questa azienda può lo stesso capire che sei tu a collegarti ad un certo sito, basandosi su altri dati pubblici che sono comunque a sua disposizione.

EVITARE IL TRACCIAMENTO DEL TUO PROVIDER E DEL SERVER

Ogni volta che ti colleghi ad internet ti viene assegnato un indirizzo IP (4 numeri separati da dei puntini). Ricordi?

Attraverso l'indirizzo IP è possibile rintracciare una persona in modo molto preciso. Gli IP vengono infatti assegnati dal tuo "provider" (l'azienda che ti dà la connessione ad internet). Inoltre sono univoci: non esistono due computer collegati in rete che abbiano indirizzi IP uguali.

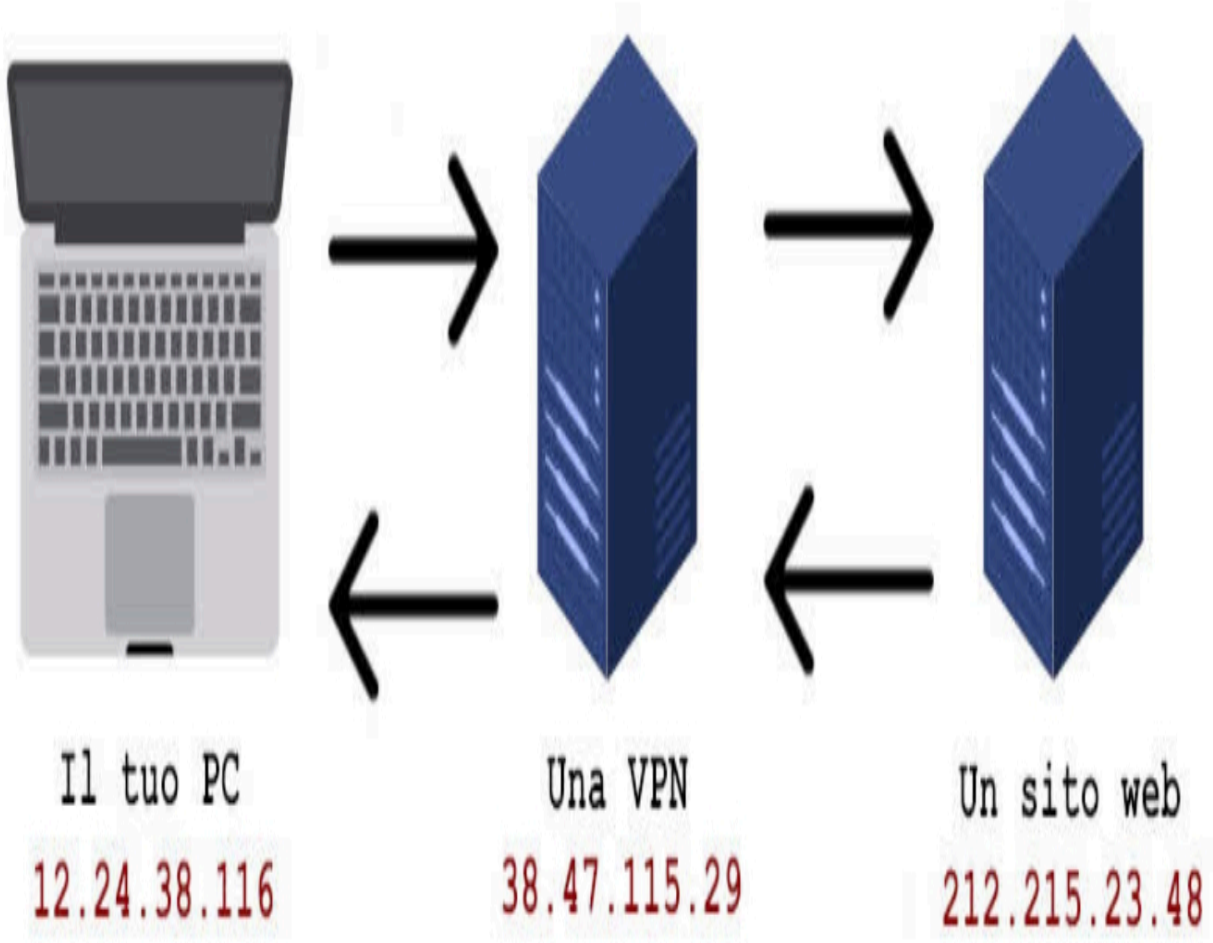
Se ti colleghi in una scheda anonima del browser, sei disconnesso dal tuo account Google e usi un servizio internet (come ad esempio Facebook) per insultare o minacciare qualcuno, sarà comunque possibile risalire alla tua identità. Il servizio infatti sa da quale indirizzo IP ti sei collegato, e partendo da questo dato è possibile chiedere al provider i dati della persona che ha stipulato il contratto.

Per "toccare con mano" l'enorme quantità di informazioni che un server può vedere quando ti ci colleghi, vai su questo sito:

infobyip.com

Per nascondere ai server queste informazioni (anche se solo parzialmente), devi utilizzare una VPN. Le VPN sono servizi internet che fanno da "intermediario" tra te ed i server degli altri servizi internet.

In pratica, tu ti colleghi alla VPN, ed è la VPN a fare le richieste ai server ed a girarti la risposta.



ATTENZIONE: affinché il giochetto funzioni, è necessario che la VPN sia "sicura". In altre parole, devi essere certo che:

- Il tuo indirizzo IP venga davvero mascherato
- La VPN abbia una “no log policy”: significa che non deve memorizzare da nessuna parte il tuo vero indirizzo IP

Scegli accuratamente la tua VPN ed evita quelle gratuite: molto spesso per finanziarsi raccolgono i tuoi dati personali, mandando quindi a quel paese l’anonimato.

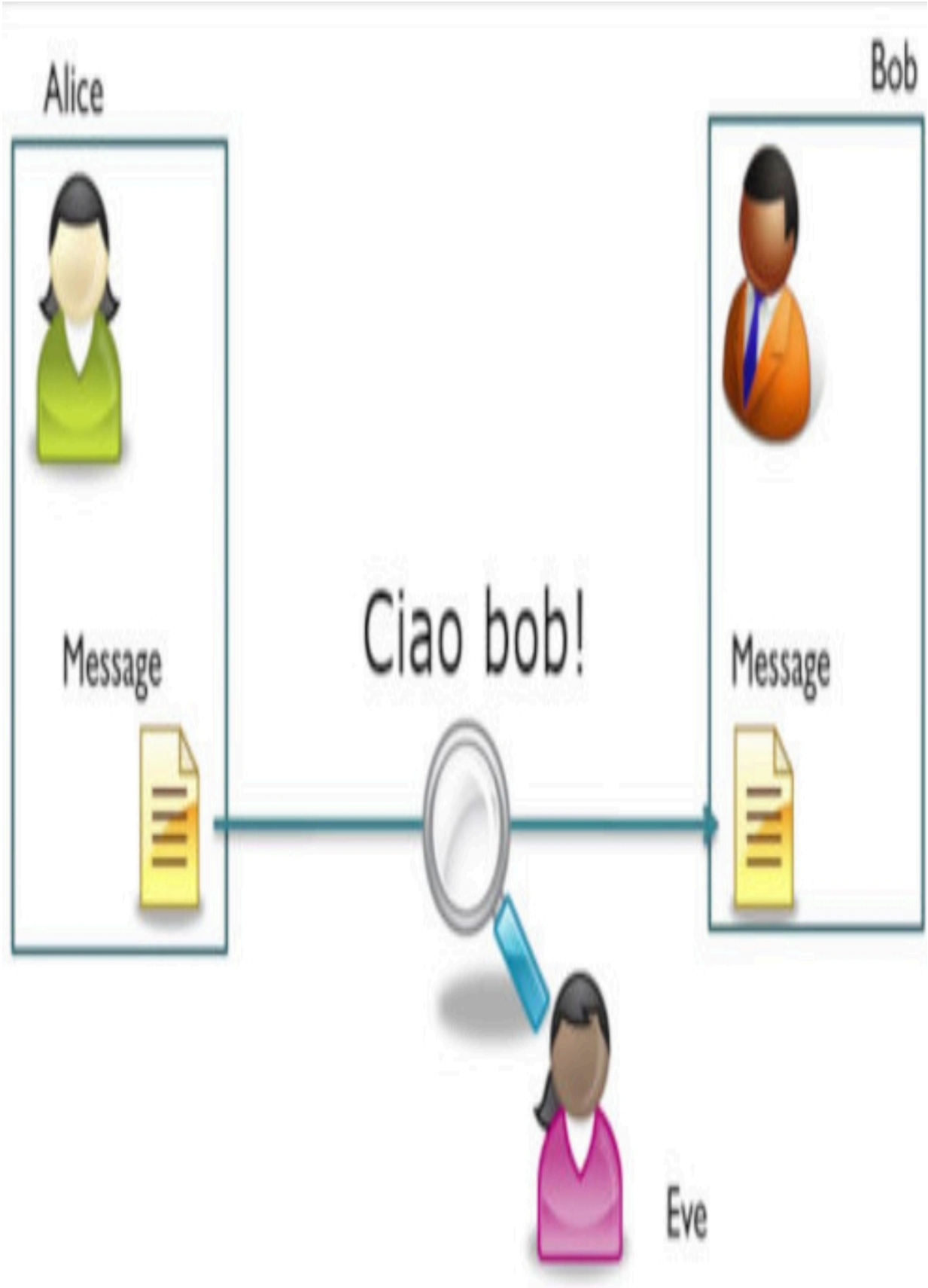
Ora che il tuo IP è mascherato il tuo provider non sarà in grado di capire quali servizi usi quando ti colleghi ad internet. E nemmeno i server: registreranno le visite come se provenissero dall’IP della VPN e non dal tuo indirizzo vero.

Ora dovrei passare a spiegarti cos'è HTTPs ma non posso farlo se prima non ti spiego la crittografia.

COS'È LA CRITTOGRAFIA?

La crittografia è forse il concetto chiave per comprendere tutta la sicurezza informatica. Te lo spiego con un esempio. Considera tre persone:

- Alice, la ragazza di Bob
- Bob, il ragazzo di Alice
- Eve, un’impicciona


Alice
Bob
Message
Ciao bob!
Message
Eve

I nomi non sono casuali: Alice comincia con la “A”; Bob comincia con la “B”. Alice e Bob sono chiamati così perché i loro nomi iniziano con A e B. “Eve” si chiama così perché il nome assomiglia all'abbreviazione del termine “eavesdropper”, che in inglese significa “impiccione” o, più precisamente, “intercettatore”.

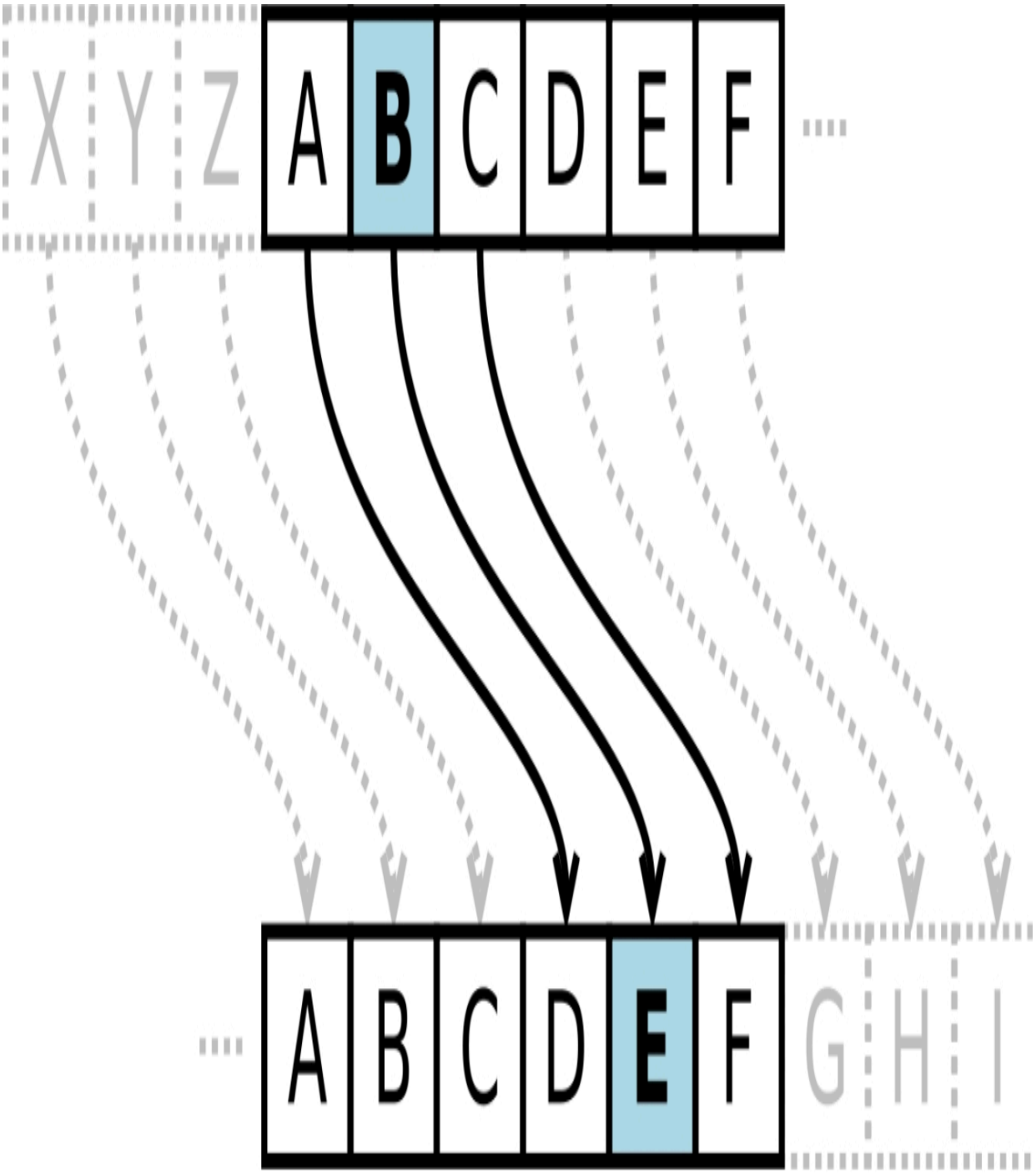
Essendo amanti, Alice e Bob vogliono comunicare senza che Eve sia in grado di capire cosa si dicono. Non si può impedire ad Eve di intercettare i messaggi, quindi l’unica soluzione possibile è quella di renderli leggibili solo da Alice e Bob.


Alice
Bob
Message
HGhhs54%%s
Message
Eve

La crittografia (o cifratura) è un procedimento matematico che rende un testo leggibile solo dal possessore di una chiave. La chiave può anche essere anche chiamata “cifrario”.

Troppo complicato da capire? Niente affatto! La crittografia non è un concetto legato ai computer o all'informatica. Esiste da secoli.

Il “cifrario di Cesare” è probabilmente l'algoritmo di cifratura più antico di cui siamo a conoscenza. La "chiave" consiste semplicemente di un numero, ad esempio 3. Per cifrare un messaggio devi usare la lettera 3 posizioni avanti nell’alfabeto, mentre per decifrarlo devi usare la lettera 3 posizioni indietro.



Ad esempio, il nome “Danilo Cimino” cifrato col cifrario di Cesare e con chiave 3 è:

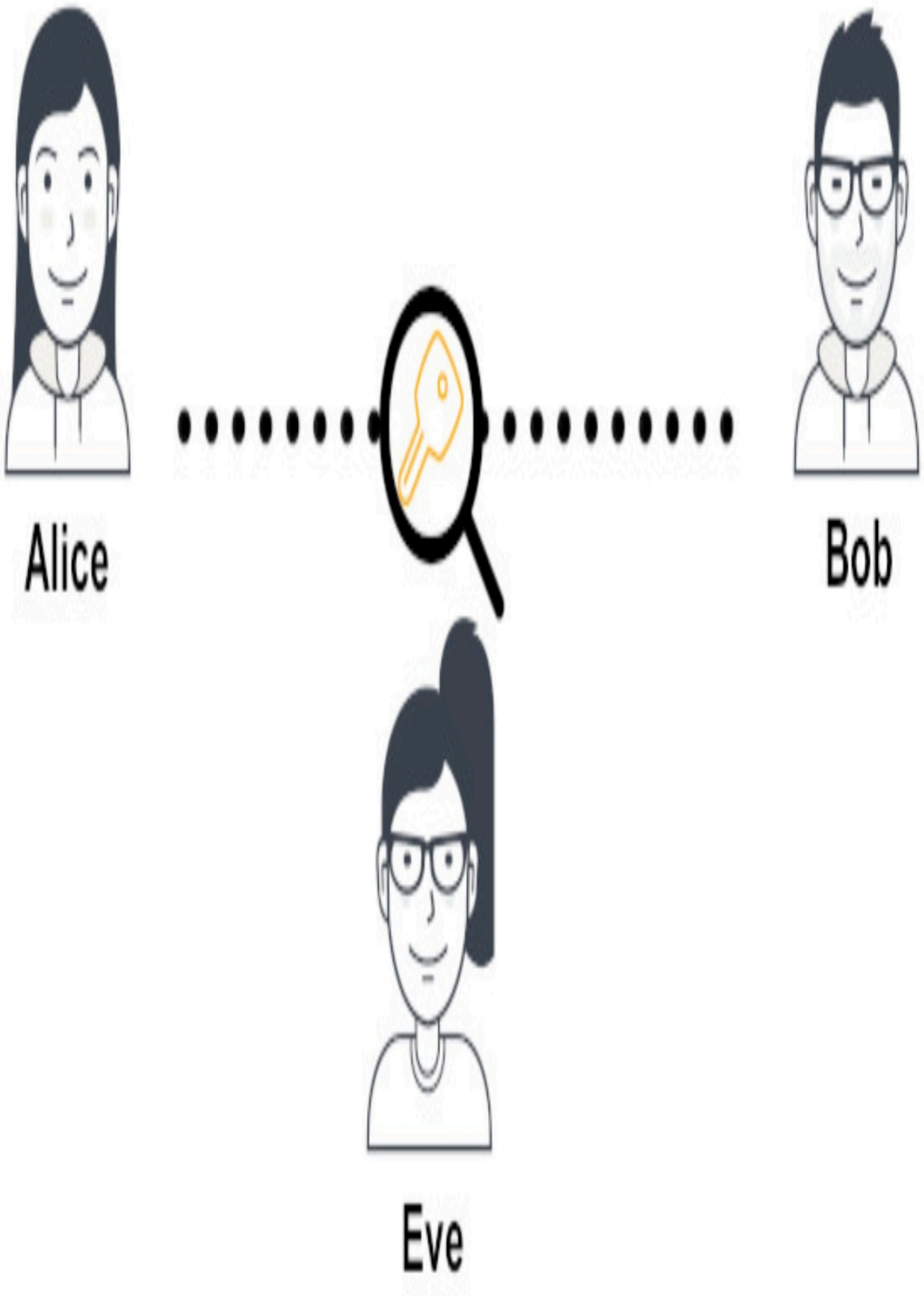
Gdqnor Fnpnqr

Non è molto difficile indovinare la chiave di un messaggio crittografato col cifrario di Cesare. Però usarlo potrebbe essere sufficiente a scoraggiare un buon numero di persone dal tentare di decifrarlo. Di sicuro è molto meglio che usare un testo completamente in chiaro.

Il cifrario di Cesare ha un difetto enorme: è basato su un'informazione condivisa. In altre parole, mittente e destinatario condividono un segreto, ovvero la chiave.

All'epoca dei romani il cifrario di Cesare poteva anche essere efficace. Ai giorni nostri però non possiamo permetterci di usarlo per proteggere i messaggi inviati su internet, per un motivo banale: bisognerebbe prima trasmettere la chiave.

Se Alice volesse comunicare con Bob, dovrebbe infatti prima mandargli un messaggio contenente la chiave. Questo messaggio verrebbe intercettato da Eve, rendendo quindi inutile l'operazione di cifratura.


Alice
Bob
Eve

Come si può risolvere il problema? Semplicemente togliendo di mezzo l'informazione condivisa, utilizzando la crittografia a chiave pubblica.

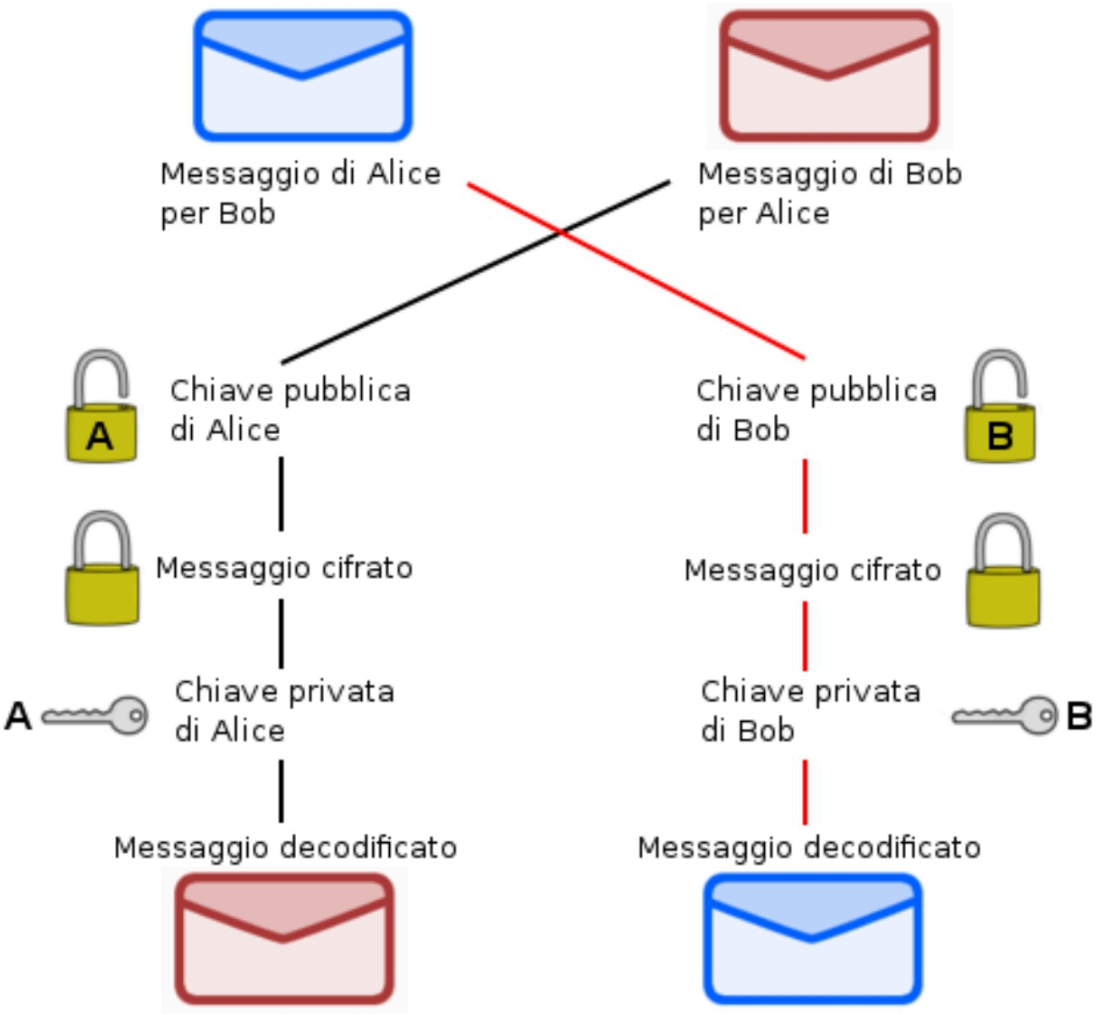
COS'È LA CRITTOGRAFIA A CHIAVE PUBBLICA?

La crittografia a chiave pubblica (o asimmetrica) è un espediente matematico che evita il problema del segreto condiviso. Si basa sulla presenza di due chiavi:

- Chiave pubblica
- Chiave privata

Quando Alice vuole inviare un messaggio a Bob, lo cifra usando la chiave pubblica di Bob. Dopo aver ricevuto il messaggio cifrato, Bob lo potrà decifrare usando la sua chiave privata.

Questo sistema si basa su un trucco matematico abbastanza complicato. Talmente complicato che solo pochissimi matematici al mondo sono in grado di comprenderlo. Il segreto del suo funzionamento sta nel fatto che solo la chiave privata di Bob può decifrare un messaggio cifrato con la chiave pubblica di Bob.



Il capostipite degli algoritmi di cifratura a chiave asimmetrica si chiama RSA e prende il nome dai tre matematici che lo hanno inventato: Ronald Rivest, Adi Shamir e Leonard Adleman. E' alla base di PGP (“Pretty Good Privacy”, “ottima privacy”), una famiglia di software che gestisce la crittografia applicata all'autenticazione ed alla privacy degli utenti.

Non hai bisogno di conoscere PGP, RSA o il cifrario di Cesare per navigare in modo anonimo. Devi però sapere cos'è la crittografia, sapere come protegge la tua privacy e riconoscere i canali cifrati su internet. Comunque ormai quasi tutti i servizi internet funzionano comunicando su connessioni cifrate senza che tu nemmeno te ne accorga.

Ora ti spiegherò un concetto che ti farà capire immediatamente come la crittografia può rendere la navigazione sul web "sicura".

COS'È HTTPS?

Ti sarà sicuramente capitato di incappare nel messaggio "la connessione non è privata". Cosa vuol dire esattamente?

La connessione non è privata

Gli utenti malintenzionati potrebbero provare a carpire le tue informazioni da **www**[redacted] (ad esempio, password, messaggi o carte di credito).

Ulteriori informazioni

NET::ERR_CERT_AUTHORITY_INVALID

Internet è una rete di computer che offre servizi, ricordi? Quando apri un browser e digiti qualcosa, stai usando il servizio "web". Ecco quello che succede:

- Il tuo computer (o il tuo cellulare) chiede ad un server di mostrargli una certa pagina

- Il server risponde con la pagina che hai richiesto


Browser web
(client)
Server web
richiesta
risposta

Ora supponi di volerti collegare al sito della tua banca. Per accedere, devi come minimo inserire la tua mail e la tua password. Ma cosa succede se un intruso si mette in ascolto sul canale di comunicazione tra il tuo computer ed il server della banca? Semplice: l'intruso sarà in grado di intercettare le tue credenziali di accesso, proprio come nel caso di Alice, Bob ed Eve.

Per evitare che qualcuno riesca a svuotarti il conto corrente, bisogna che il canale sia cifrato con la crittografia a chiave pubblica.

HTTPS è il nome di un protocollo di comunicazione che protegge i dati scambiati tra il tuo computer ed i siti web che visiti. In altre parole, rende la connessione "sicura" nel senso che nessun intruso sarà in grado di leggere i dati che vi passano attraverso.

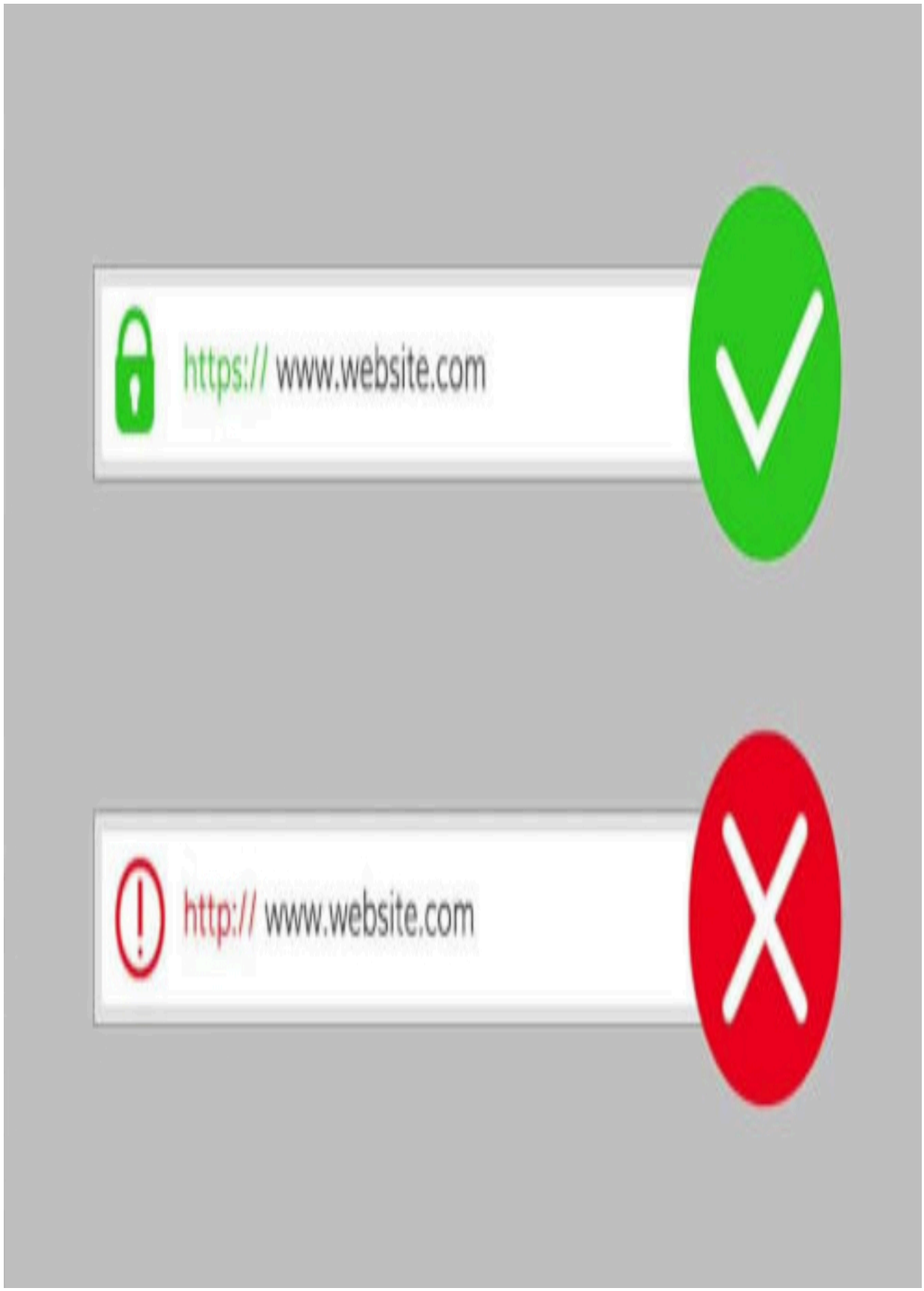
Per sapere se un sito è sicuro, guarda la barra dell'indirizzo del browser. Se l'indirizzo inizia con:

https://

Allora è "sicuro" (la connessione è cifrata). Se invece leggi solo:

http://

Allora il sito non è "sicuro" (la connessione non è cifrata). Puoi anche visitarlo ma devi evitare di autenticarti o di inserire informazioni in qualunque casella di testo. In altri termini: leggi pure il contenuto del sito ma non scriverci nulla.


https:// www.website.com
http:// www.website.com

ATTENZIONE! Esistono siti che:

- Usano HTTPS ma NON SONO SICURI
- NON usano HTTPS ma sono SICURISSIMI

HTTPS non garantisce che andando su un sito tu non possa beccare un virus. Garantisce solo che il canale di comunicazione sia cifrato, quindi a prova di intercettazione.

Ad esempio, il sito del cerchio Firenze 77 non usa HTTPS ma è sicurissimo. Semplicemente, è stato creato in un'epoca in cui HTTPS non esisteva e, non essendo più aggiornato, nessuno si è preso la briga di aggiungere il supporto a questo protocollo.

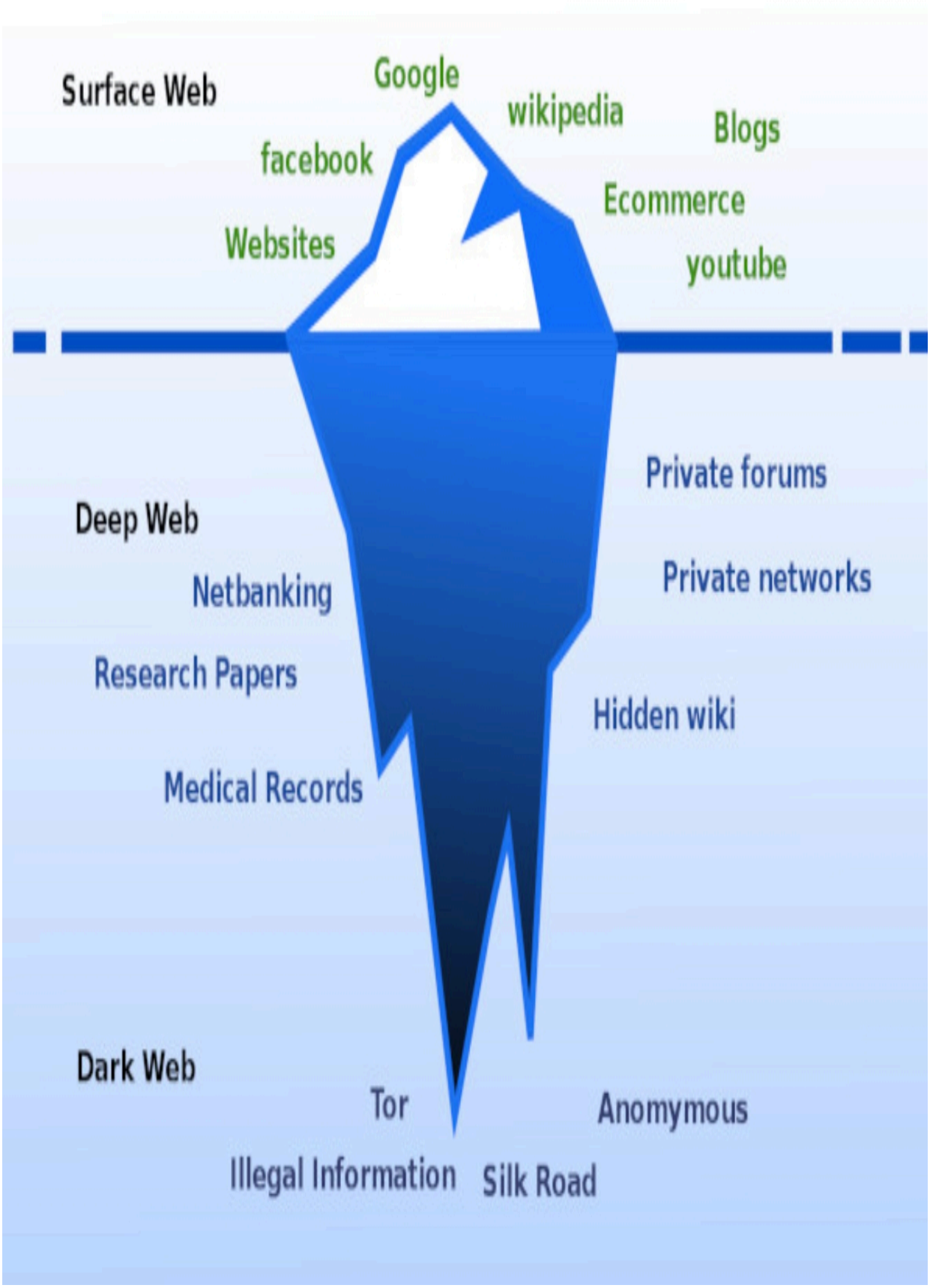

Non sicuro – cerchiofirenze77.org
Cerchio Firenze 77
Cos'è il Cerchio Firenze 77 (Storia della medianità di Roberto Setti)
Cosa si propone il Cerchio

COSA SONO DEEP WEB E DARK WEB?

Ora entreremo meglio nel vivo dell'argomento di questo manuale. Quello che ti ho spiegato finora è necessario a capire bene tutto quello che seguirà. Però non è necessario che tu ricordi tutto a memoria: se ti sfugge qualcosa, torna indietro e leggi il paragrafo dedicato.

Il deep web è costituito da tutte la pagine raggiungibili immettendo delle credenziali di accesso (tipicamente email e password). Ad esempio il sito web della tua banca, che ti mostra il saldo e la lista dei movimenti del tuo conto corrente. Le pagine del deep web non sono anonime o pericolose: vengono semplicemente escluse dai motori di ricerca.

Il dark web invece è un insieme di siti raggiungibili solo attraverso una “darknet” (“rete oscura”). Una darknet può essere vista come una rete "sovrapposta" ad internet, pensata per farti restare nell’anonimato più totale. Ecco una rappresentazione schematica di tutto il web:


Surface Web
Google
wikipedia
Blogs
facebook
Ecommerce
Websites
youtube
Private forums
Deep Web
Private networks
Netbanking
Research Papers
Hidden wiki
Medical Records
Dark Web
Tor
Anomymous
Illegal Information
Silk Road

Sul web "di superficie" troviamo i siti “normali”. Si tratta di siti:

- Pubblici
- Indicizzati dai motori di ricerca
- Visitabili con un qualunque browser web

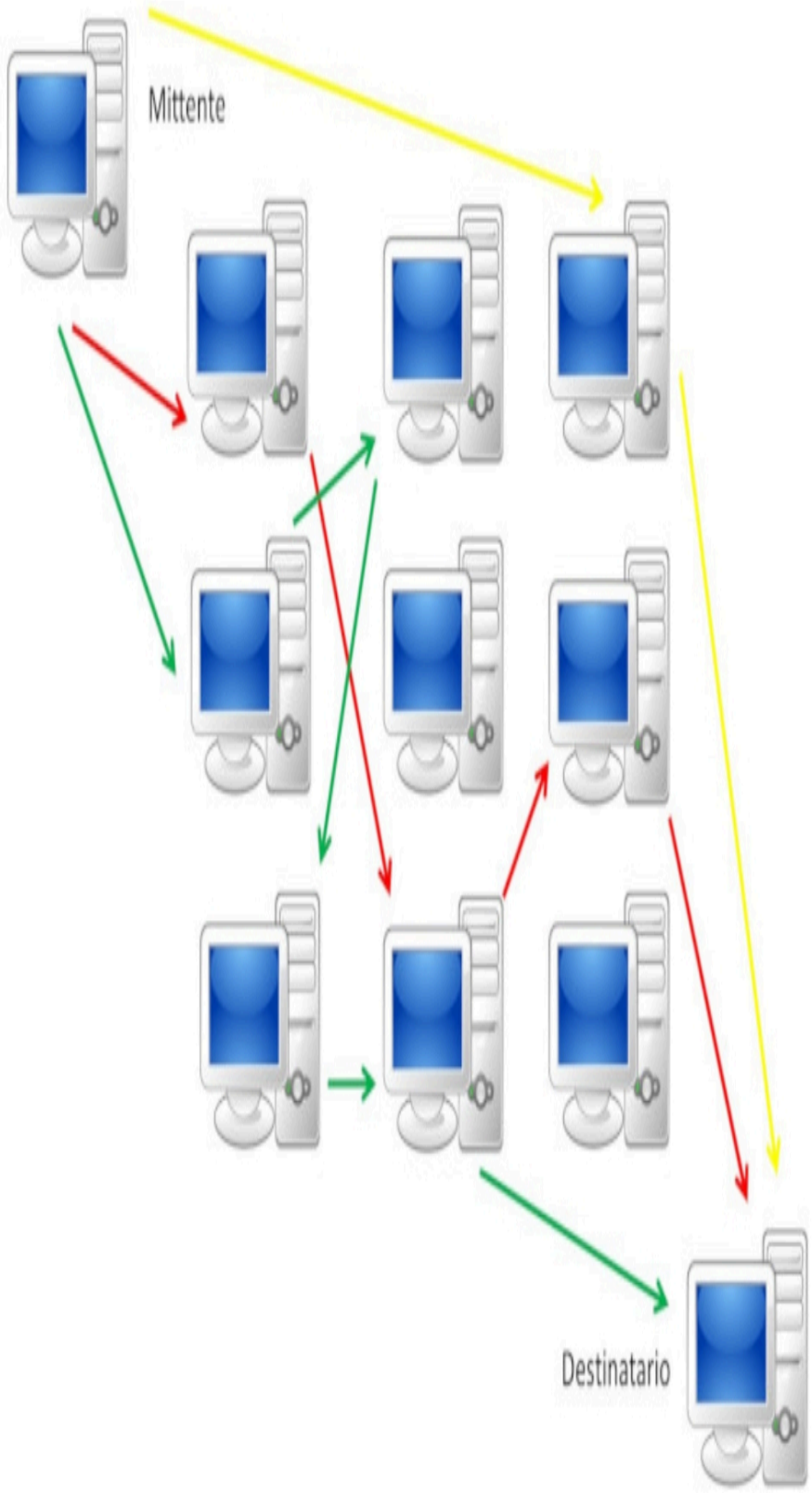
Sotto la linea blu troviamo tutti i siti di internet banking, i registri medici, i forum privati, gli articoli scientifici eccetera. Ovvero, tutte le pagine:

- Private
- Non indicizzate dai motori di ricerca
- Visitabili con un qualunque browser web ma solo dopo aver effettuato un'autenticazione (ovvero aver inserito email e password, nella maggior parte dei casi)

Più sotto ancora c’è il dark web, raggiungibile solo attraverso una “darknet”. Si tratta di pagine:

- Pubbliche
- Non indicizzate dai motori di ricerca
- Non visitabili con qualunque browser web

Le darknet sono reti pensate per fornire un anonimato totale. In teoria è impossibile essere rintracciati, perché la connessione viene smistata attraverso diversi computer (chiamati “nodi”), e sempre su percorsi diversi.


Mittente
Destinatario

In pratica però è possibilissimo essere rintracciati anche se si usa una darknet, e più avanti vedremo esattamente come e perché.

In soldoni, la faccenda è questa: finché non fai nulla di illegale, nessuno si prenderà mai la briga di rintracciarti ed il tuo anonimato sarà garantito al 100% (nel senso che i siti che visiti non sapranno mai chi sei).

In caso contrario, sappi che esistono tecniche molto efficaci per rintracciare i malintenzionati e che molto spesso trovare un criminale in rete è solo questione di quanto tempo e denaro sono disposte ad investire le forze dell'ordine.

Ciò d'altronde è vero anche per i crimini che vengono commessi nel mondo reale: essere online non cambia affatto questo stato di cose.

Ora vedremo quali sono le principali credenze errate ed i miti da sfatare sul deep web e sul dark web.

Dark web e deep web sono la stessa cosa

Falso. Il deep web è l'insieme dei siti raggiungibili dopo aver immesso delle credenziali di accesso. Il dark web è l'insieme dei siti raggiungibili usando una darknet.

Sul dark web si trovano cose raccapriccianti

Vero. Intanto però va detto che nel dark web ci sono anche moltissimi siti assolutamente legittimi ed interessanti (te ne proporrò un elenco più avanti).

Ma una buona fetta di contenuti (più del 60% secondo uno studio della Carnegie Mellon University) contiene solo cose illegali: siti che vendono droga, armi, passaporti, soldi falsi ed altre amenità del genere.

Purtroppo c’è anche tantissimo materiale pedopornografico o comunque disturbante. Ti consiglio di starne alla larga, anche se vuoi visionare questi materiali per pura curiosità: c’è il rischio di incappare in qualche malware o in un controllo delle forze dell’ordine, che quasi certamente monitorano

costantemente il dark web e potrebbero male interpretare lo scopo della tua visita.

Non esistono motori di ricerca per il dark web

Esistono eccome. Solo che non funzionano bene come Google. Più avanti ti spiegherò come fare a cercare informazioni nel dark web.

Il dark web è stato inventato dalla CIA

Falso ma "quasi" vero. La rete TOR (una darknet che esaminerò dettagliatamente più avanti) è stata creata dalla marina degli stati uniti per proteggere le comunicazioni dei servizi segreti.

Il dark web è una trappola della CIA per catturare i criminali

Falso. Le darknet, come vedremo meglio più avanti, sfruttano la crittografia a chiave pubblica. Pertanto è impossibile che la CIA, la NSA o qualunque altro ente simile possa "spiare" il traffico che vi passa usando una "chiave universale" di decifratura. Non è proprio tecnicamente possibile. Se la cosa non ti torna, rileggi il capitolo dedicato alla crittografia a chiave asimmetrica.

Molti pensano: "se il deep web è stato creato dalla CIA, allora la CIA ne possiede le chiavi". Sbagliato. Il muratore che ha costruito la casa in cui abiti possiede le chiavi di casa tua, per caso?

Il dark web è molto più grande del web di superficie

Falso. Per molto tempo si è creduto che i siti del dark web fossero molti di più di quelli del web di superficie ma in realtà non è così. Una ricerca di Recorded Future (un’autorevole azienda di “intelligence”, ovvero di analisi delle informazioni) ha svelato finalmente i numeri definitivi. Pare che al momento della ricerca i siti del dark web fossero 55.828, di cui solo 8.416 attivi. Molti di meno rispetto a quelli del web di superficie, che ammontano grossomodo ad 1,7 MILIARDI.

Diverso invece è il discorso che riguarda le pagine del deep web: sono sicuramente molte di più di quelle del web di superficie ma, semplicemente, non ha senso contarle.

Ti faccio un esempio: le pagine dei profili Facebook sono tutte uguali, per quanto riguarda l'impostazione grafica. Quello che cambia è solo il contenuto, diverso da un'utente all'altro: foto profilo, informazioni eccetera. Dal punto di vista tecnico la pagina del profilo di Facebook è una sola, nel senso che è stata programmata una sola volta. Quindi non ha molto senso affermare che esistono circa 2 miliardi di pagine di profilo di Facebook. È più corretto dire che Facebook ha circa 2 miliardi di utenti.

Basta una VPN e sei anonimo

Vero e falso: dipende da cosa intendi con il termine "anonimo". La VPN si occupa di mascherare il tuo indirizzo IP, evitando (come ho già detto) il tracciamento del tuo provider e dei server. Usare una darknet ti dà un grado di anonimato molto più elevato.

TOR non è altro che due VPN a cascata

Falsissimo. TOR è una darknet, una VPN è una VPN. Sono due cose diverse. Più avanti spiegherò meglio come funzionano le darknet.

Non esiste anonimato su internet

Esiste eccome! Dipende da quello che devi fare. O meglio: dipende da quale tipo di tracciamento vuoi difenderti. Ricorda sempre che, come già detto, finché non fai nulla di illegale mai nessuno si prenderà la briga di venirti a cercare, e l'anonimato sarà garantito.

La modalità in incognito basta e avanza per essere anonimi

Falso! Una persona che fa questa affermazione non ha la più pallida idea di cosa stia parlando. La modalità di navigazione in incognito impedisce solo il tracciamento del browser, facendo in modo che le pagine che visiti non vadano a finire dentro alla cronologia.

COSA SONO LE DARKNET?

Come già accennato, una darknet è una rete pensata per farti navigare in modo anonimo. Approfondisco un po' questo concetto.

Una darknet può essere vista come una rete "sovrapposta" ad internet, pensata per renderti anonimo e non rintracciabile. Usare una darknet è anche l'unico modo per accedere al dark web (non puoi entrarci usando una VPN).

Esistono circa una dozzina di darknet, contando anche quelle al momento inattive. Le più rilevanti si chiamano:

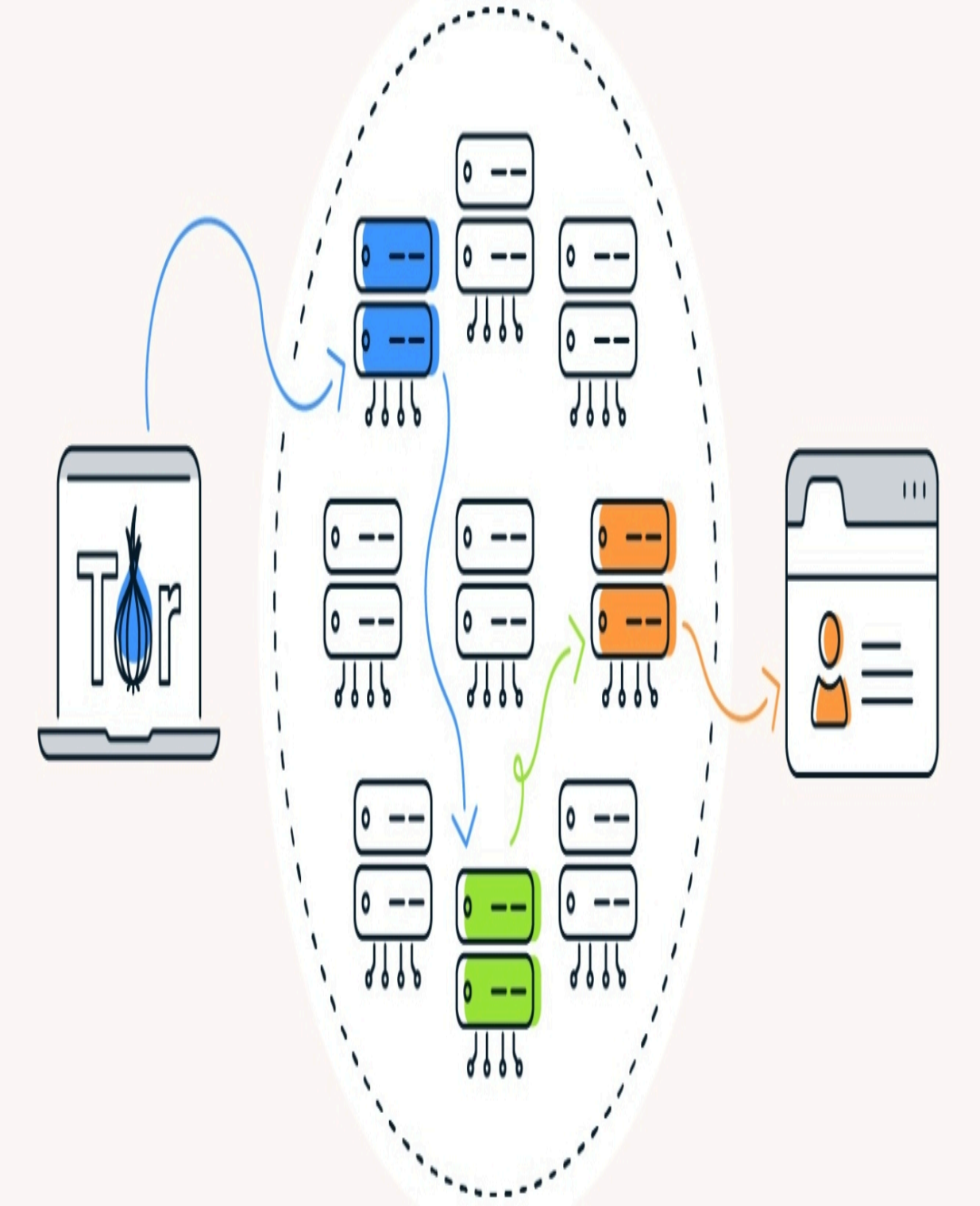
- TOR (The Onion Router, "instradatore a cipolla")
- I2P ("Invisible Internet Project", "Progetto Internet Invisibile")
- Freenet ("rete libera")

In questo manuale esaminerò solo TOR, perché è la darknet più utilizzata. Inoltre, capire come funziona TOR ti darà la giusta "apertura mentale" per capire anche come utilizzare le altre in completa autonomia (se lo vorrai).

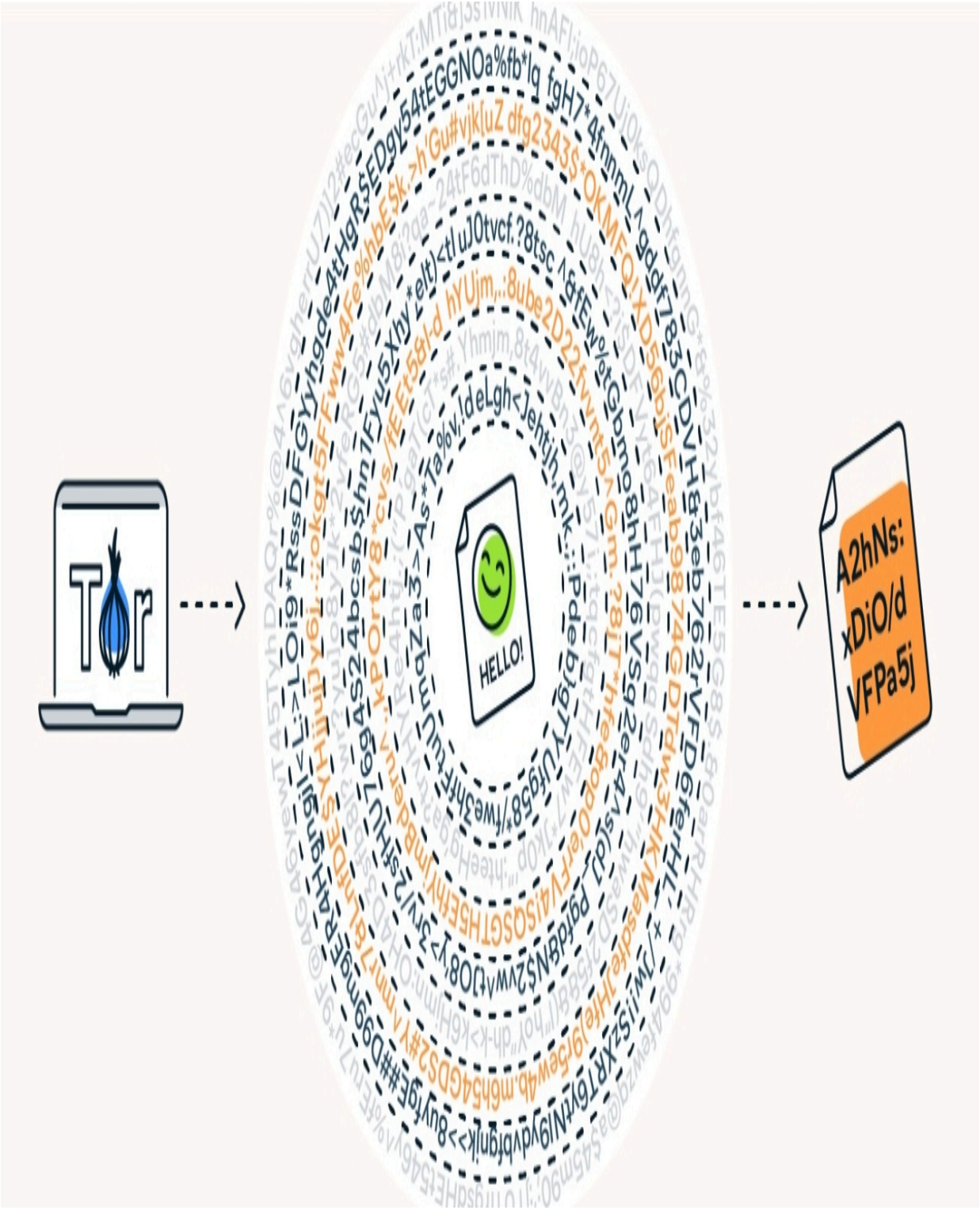
COS'È TOR?

Come già detto, TOR è una sigla che vuol dire "The Onion Router", traducibile come "instradatore a cipolla". Un nome abbastanza singolare ma che ne esprime in pieno la modalità di funzionamento, che si può riassumere così:

- Il tuo computer si collega ad un altro computer chiamato “entry node” (nodo di ingresso)
- Il tuo traffico viene “instradato” attraverso alcuni altri computer (nodi) intermedi
- Contemporaneamente, il traffico viene anche crittografato con un algoritmo a chiave asimmetrica
- Il traffico arriva poi ad un “exit node” (nodo di uscita) e da lì prosegue verso la sua destinazione



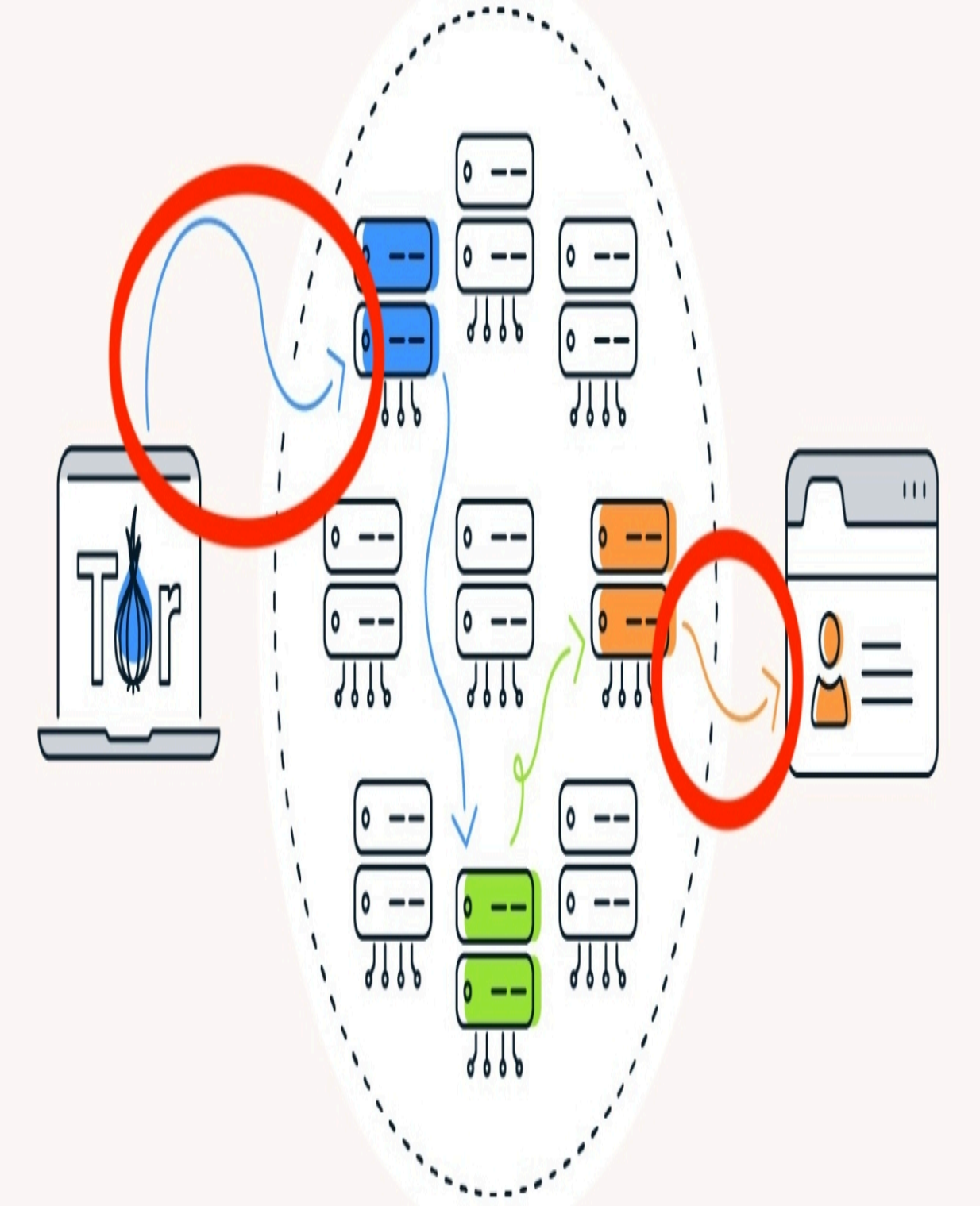
È come se il traffico attraversasse gli strati di una cipolla, venendo continuamente crittografato durante il percorso. Quando raggiunge la destinazione, l'origine del traffico è completamente sconosciuta.



TOR è lo stato dell'arte dell'anonimato su internet. Non esiste nulla di più sicuro. Questo però non vuol dire che usandolo tu sia completamente anonimo e non rintracciabile.

QUALI SONO LE VULNERABILITÀ DI TOR?

Il principale punto debole di TOR consiste nel fatto che il traffico viene nascosto solo dopo essere "entrato nella cipolla", ovvero nel percorso che compie dal nodo di ingresso al nodo di uscita. Prima di entrarvi, deve raggiungere il nodo di ingresso. E prima di raggiungere la destinazione, deve anche attraversare il percorso che lo separa dal nodo di uscita.



Questo offre ad uno "spione" tutta una serie di possibilità.

Potrebbe ad esempio fare un "attacco di correlazione". Te lo spiego raccontandoti un fatto realmente accaduto. Viene spedito un allarme bomba da uno studente universitario, attraverso TOR ma collegandosi alla WiFi dell'università. La polizia chiede all'ateneo di dargli l'elenco delle connessioni fatte tramite TOR nel giorno e nella fascia oraria della ricezione dell'allarme bomba. Vengono identificati tre studenti. La polizia li interroga tutti e tre ed uno di loro confessa.

La polizia non è riuscita a vedere il traffico ma attraverso l'interrogatorio è riuscito a "correlare" la confessione al collegamento attraverso TOR. Quindi quando ti collegherai attraverso TOR, ricorda sempre che il tuo provider (l'azienda o l'ente che ti fornisce la connessione) riuscirà a vedere che stai usando TOR (a meno che tu non prenda le giuste contromisure, che vedremo più avanti).

Ma non finisce mica qui: lo "spione" potrebbe ad esempio assoldare un hacker per cercare di fargli prendere il controllo del nodo di ingresso, riuscendo quindi a vedere in chiaro il tuo traffico.

C'è anche un altro aspetto da considerare: i nodi di TOR sono teoricamente mantenuti da dei volontari. In pratica, molti di essi sono quasi certamente controllati dalle forze dell'ordine. E molti altri invece sono probabilmente sotto il controllo degli "hacker etici": esperti di sicurezza informatica che usano le loro competenze a fin di bene, ad esempio per rintracciare i pedofili.

COME RIMEDIARE ALLE VULNERABILITÀ DI TOR

Se vivi in un paese democratico e non hai intenzione di violare la legge, usare TOR così com'è ti garantirà un altissimo grado di anonimato (purché tu segua le indicazioni che ti darò più avanti).

Se invece abiti in un paese governato da un regime oppressivo, in cui è in vigore una legge sbagliata che viola i tuoi diritti umani, avrai bisogno di proteggerti dalle vulnerabilità di TOR. Esistono fondamentalmente 4 opzioni:

1. Usare una VPN e poi collegarti a TOR

2. Usare un TOR bridge

3. Usare la WiFi di qualcun altro (illegale)

4. Usare un cellulare con una scheda SIM anonima o intestata a qualcun altro (illegale)

Riguardo alla possibilità 1, la VPN effettivamente è una soluzione molto efficace. Essa infatti maschera il tuo vero indirizzo IP, per cui il tuo provider non saprà che ti stai collegando con TOR. E chi controlla il nodo di ingresso non verrà a conoscenza del tuo vero indirizzo IP (purché tu scelga, come detto nel capitolo dedicato alle VPN, un servizio "no log").

Il problema di questa soluzione è che è difficile da realizzare se hai intenzione di usare un sistema amnesico per neutralizzare il tracciamento del sistema operativo. Altrimenti è un'opzione abbastanza efficace.

Riguardo alla possibilità 2, i "TOR bridges" sono nodi di ingresso che non fanno parte dell'elenco pubblico di TOR. Inoltre sono protetti da un software di "offuscamento": serve a mascherare il fatto che il traffico che vi passa attraverso sia traffico sulla rete TOR.

Il problema di questi "bridges" è che non è possibile garantire la loro affidabilità: potrebbero essere sotto il controllo di hacker o forze dell'ordine, esattamente come nel caso dei nodi normali.

Le possibilità 3 e 4 sono le migliori. Risolvono il problema alla radice: se si una una linea internet intestata a qualcun altro, si fa MOLTA attenzione a non lasciare tracce durante la navigazione via TOR ed si usa un sistema amnesico, si può raggiungere la cosiddetta "plausible deniability" (negazione verosimile).

È un'espressione che viene usata per indicare quei casi in cui una persona può legittimamente dichiararsi estranea ad un fatto. Si può fare solo se non ci sono prove a carico o se quelle disponibili possono essere "verosimilmente negate".

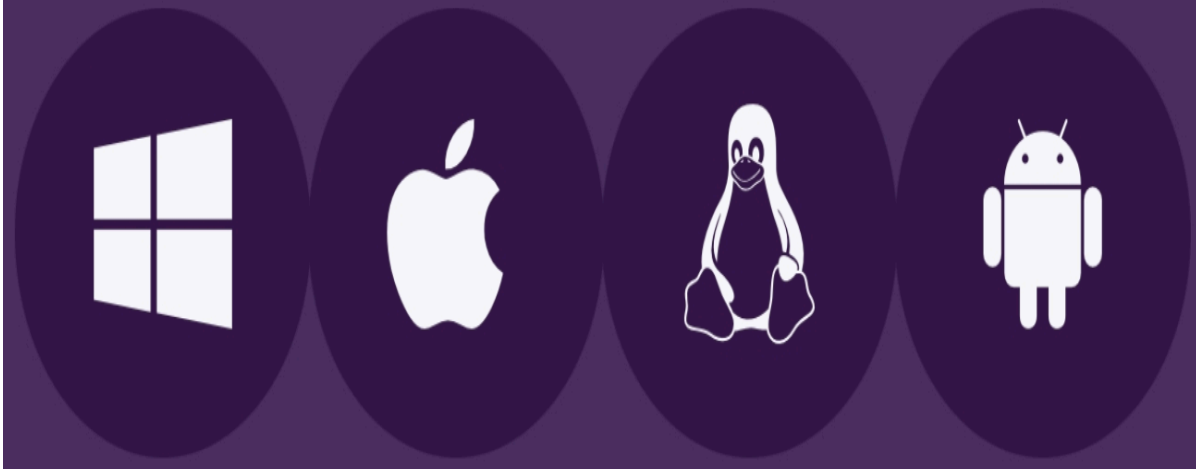
COME SI USA TOR?

È facilissimo. Non devi fare altro che andare su questo sito:

https://www.torproject.org/download/

Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.

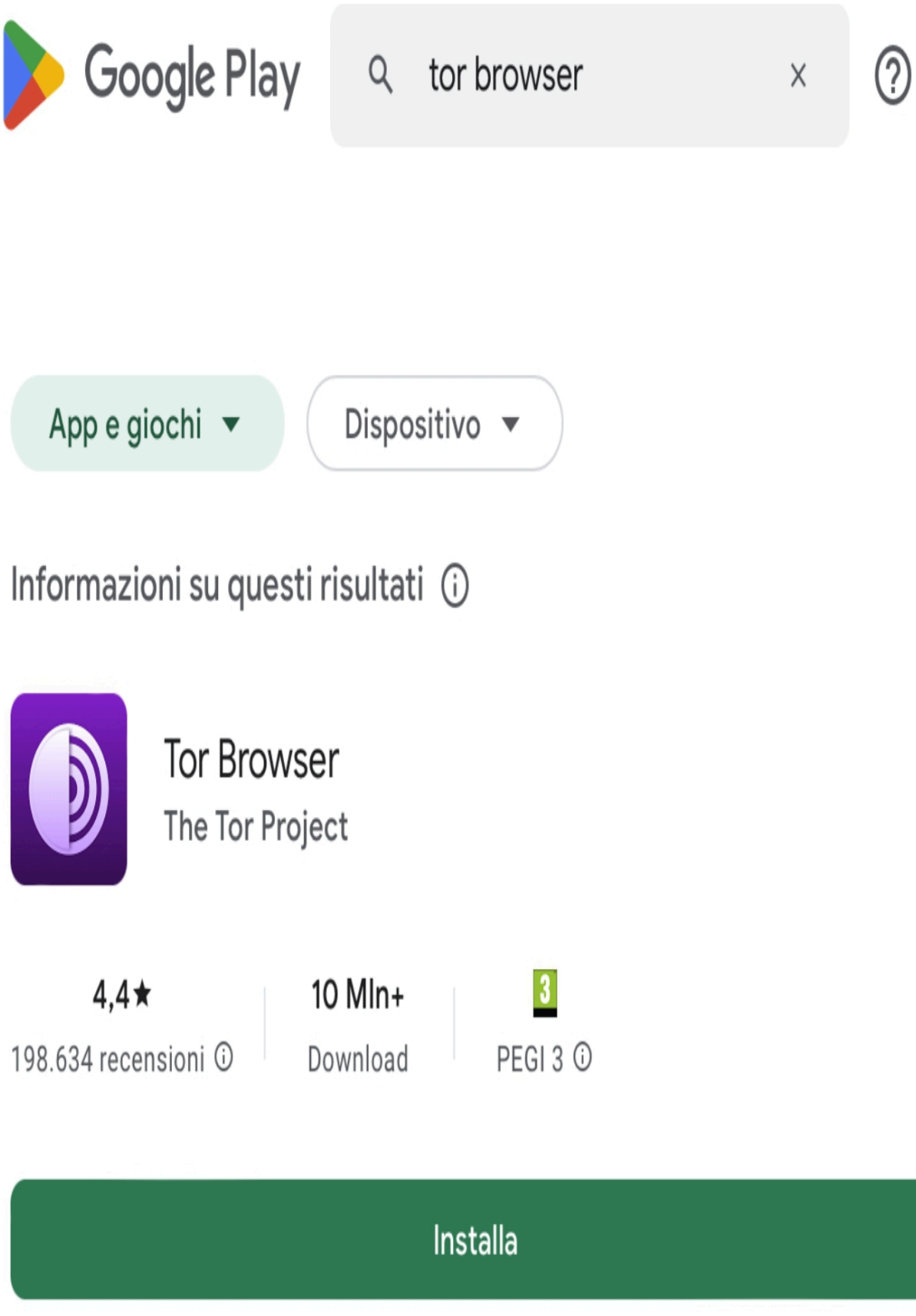


Download for Windo Download for macO Download for Linux Download for Android

Poi devi premere sull'icona del tuo sistema operativo: verrà scaricato il "TOR Browser", un browser web che farà passare tutto il traffico attraverso TOR, consentendoti anche l'accesso al dark web.

Puoi usare TOR Browser sia con un cellulare che con un PC. Si installa come una qualunque app o un qualunque programma.

È disponibile per Windows, Linux e MacOS. L'app per Android si può scaricare sia dal sito che ti ho indicato sopra che dal Google Play Store.


Google Play
tor browser
App e giochi
Dispositivo
Informazioni su questi risultati
Tor Browser
The Tor Project
4,4★
198.634 recensioni
10 Mln+
Download
3
PEGI 3
Installa

L'app per iPhone non si può scaricare dal sito: Apple non consente l'installazione di app che non siano prima state approvate dal suo staff. Pertanto, per ottenerla dovrai aprire "App Store" e scaricarla da lì. Cercando "tor browser" ti verranno fuori diversi risultati, perché non esiste un'app "ufficiale". Sul sito di TOR però viene consigliato di utilizzare l'app chiamata "onion browser", per cui digita queste parole ed installa l'app che ti esce fuori come primo risultato.

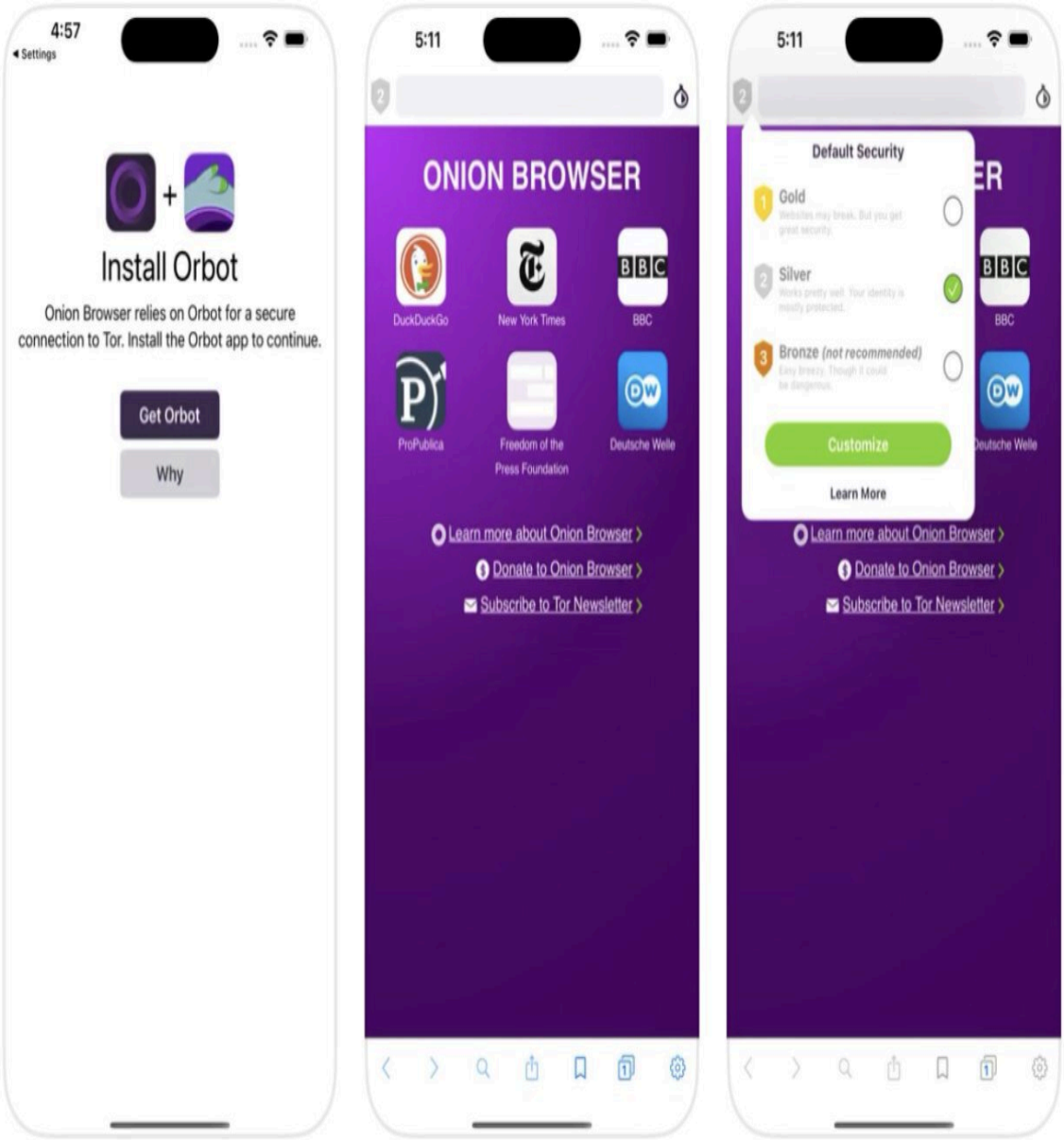
Onion Browser

Secure, anonymous web with...

★★★★☆ 127

GET

In-App Purchases



Fatto? Bene. Ora non dovrai fare altro che toccare sull'icona dell'app (nel caso di Android o iOS) o fare doppio click sull'icona del programma (nel caso di Windows o di Linux).

USARE TOR SU IPHONE

Se hai un iPhone, al primo avvio ti verrà chiesto di installare un'altra app: si chiama "Orbot". Serve a mascherare la connessione a TOR. Installerà sul tuo telefono una VPN "speciale", gratuita e pensata apposta per l'uso con TOR Browser.

Install Orbot

Onion Browser relies on Orbot for a secure connection to Tor. Install the Orbot app to continue.

Get Orbot

Why

Premi su "Get Orbot", ti si aprirà di nuovo App Store. Installa Orbot ed aprila. Premi su "Install" e poi su "Consenti". Potrebbe esserti richiesto di inserire il codice di sblocco del tuo iPhone. Fatto? Bene: ora premi su "Start".

Il robottino inizierà a saltare e dopo qualche secondo sarai connesso. Ora torna ad Onion Browser.

Orbot installed! One more step.

Ask Orbot for permission to access it.

This will allow **Onion Browser** to:

- Use Orbot to connect to the official Tor network.
- Get updates on the status of the connection.

Request Access

Why

Dovrai chiedere ad Orbot di consentirti l'accesso, premendo su "Request Access". Si aprirà di nuovo la schermata di Orbot.

Access Request

Onion Browser wants to access Orbot.

This will allow Onion Browser to:

- Get updates on the status of the connection.
- Get information about Tor circuits.
- Stop Tor.

Grant

Deny

Premi su "Grant" (significa "concedi" in italiano), poi premi su "Apri". Verrai riportato su Onion Browser.

Start Tor in Orbot.

Then come back for private browsing.

Start Tor

Why

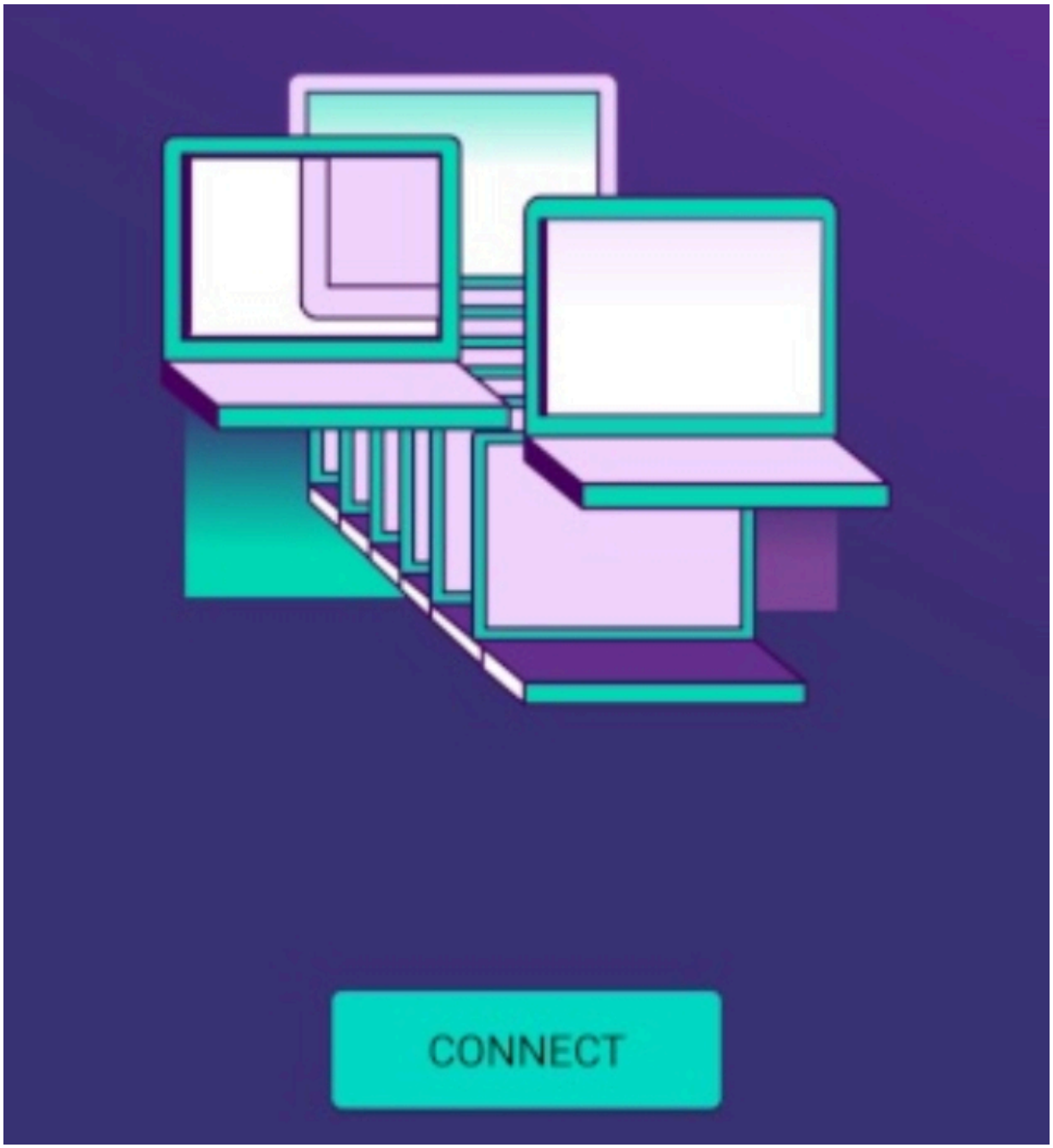
Premi su "Start Tor". Si aprirà di nuovo Orbot ed il robottino inizierà di nuovo a saltare. Quando ti sarai connesso, torna all'app Onion Browser. Da questo momento in poi potrai visitare il web di superficie in modo anonimo (la connessione verrà instradata attraverso la rete TOR). Puoi anche visitare il dark web: più avanti ti spiegherò come fare.

USARE TOR SU ANDROID

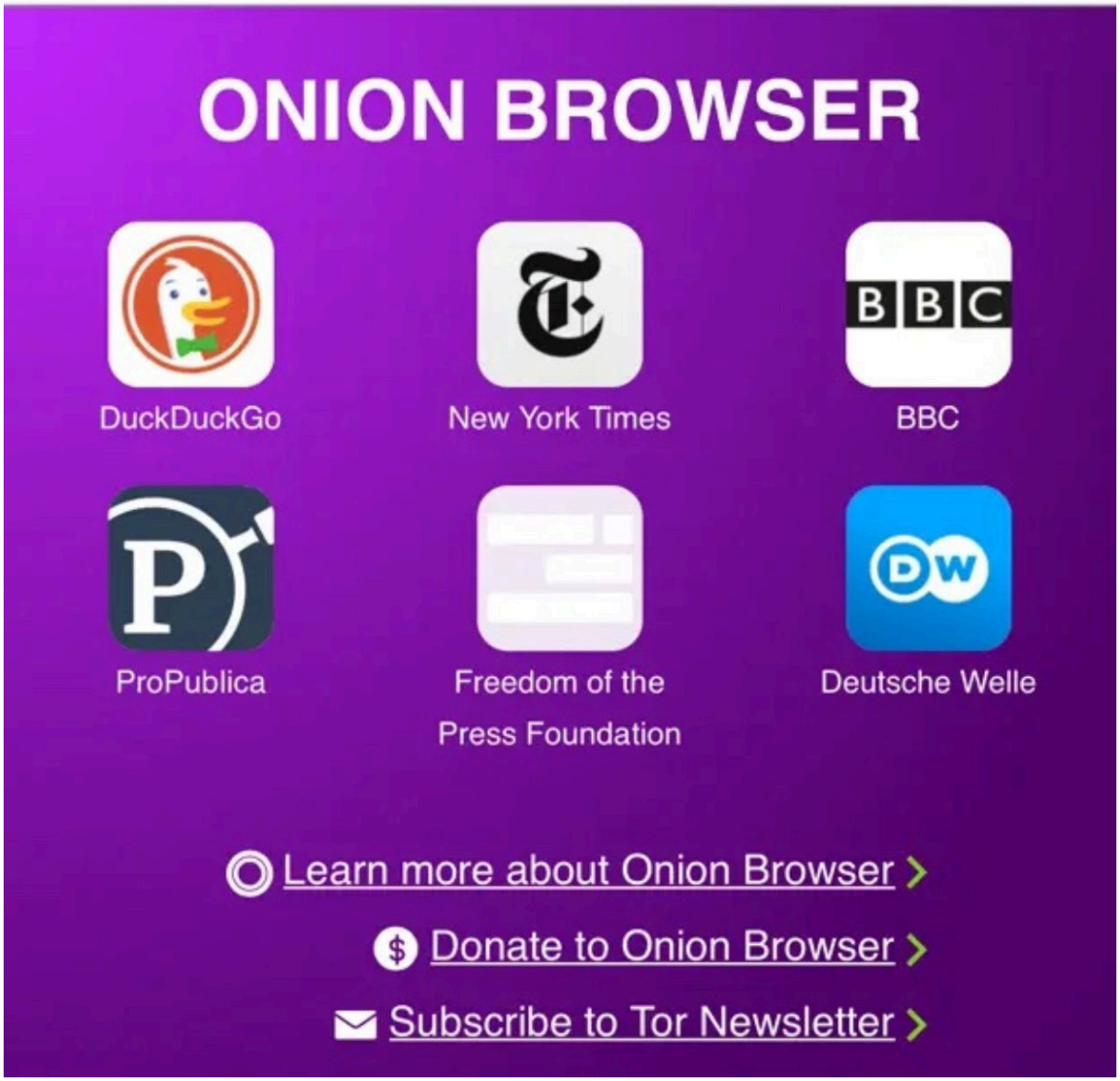
Se hai Android, il tutto dovrebbe essere più semplice. Dico "dovrebbe" perché Android viene fornito gratis ai produttori di smartphone, che hanno la libertà di modificarlo a proprio piacimento. Quindi TOR Browser potrebbe anche non funzionare: dipende da quale modello di cellulare possiedi. In alcuni casi non si riesce né ad installare e né ad avviare.

Non posso indicarti una procedura precisa di installazione o di risoluzione dei problemi. Se non riesci a connetterti, non posso fare altro che suggerirti di cercare su Google per vedere se qualcun altro col tuo stesso telefono ha già risolto il problema.

Comunque, in teoria basta avviare l'app e premere sul tasto "Connect".

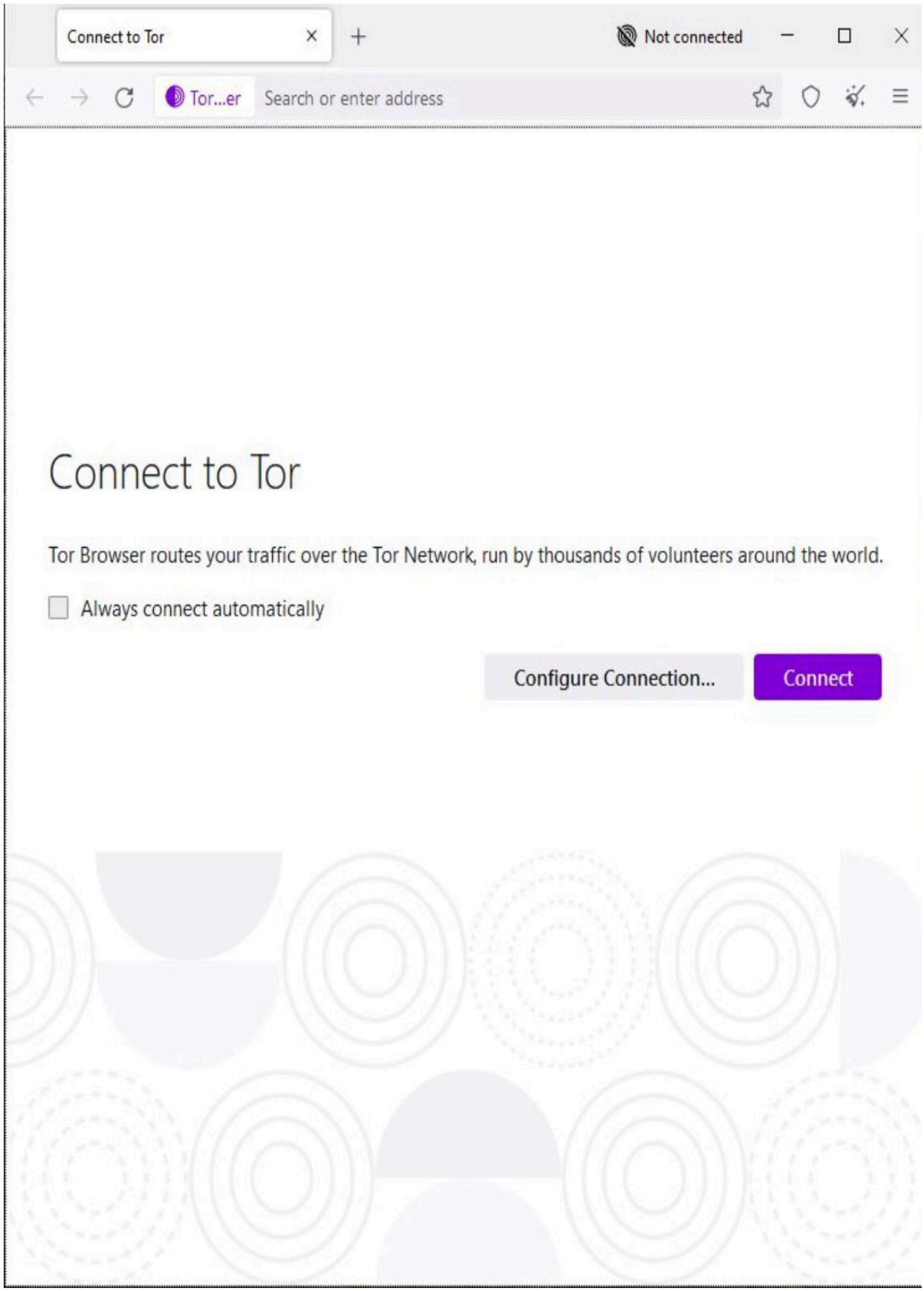


Come nel caso dell'iPhone, da questo momento in poi potrai visitare il web di superficie in modo anonimo, ma anche tuffarti nel dark web. Più avanti ti darò istruzioni più precise in merito.

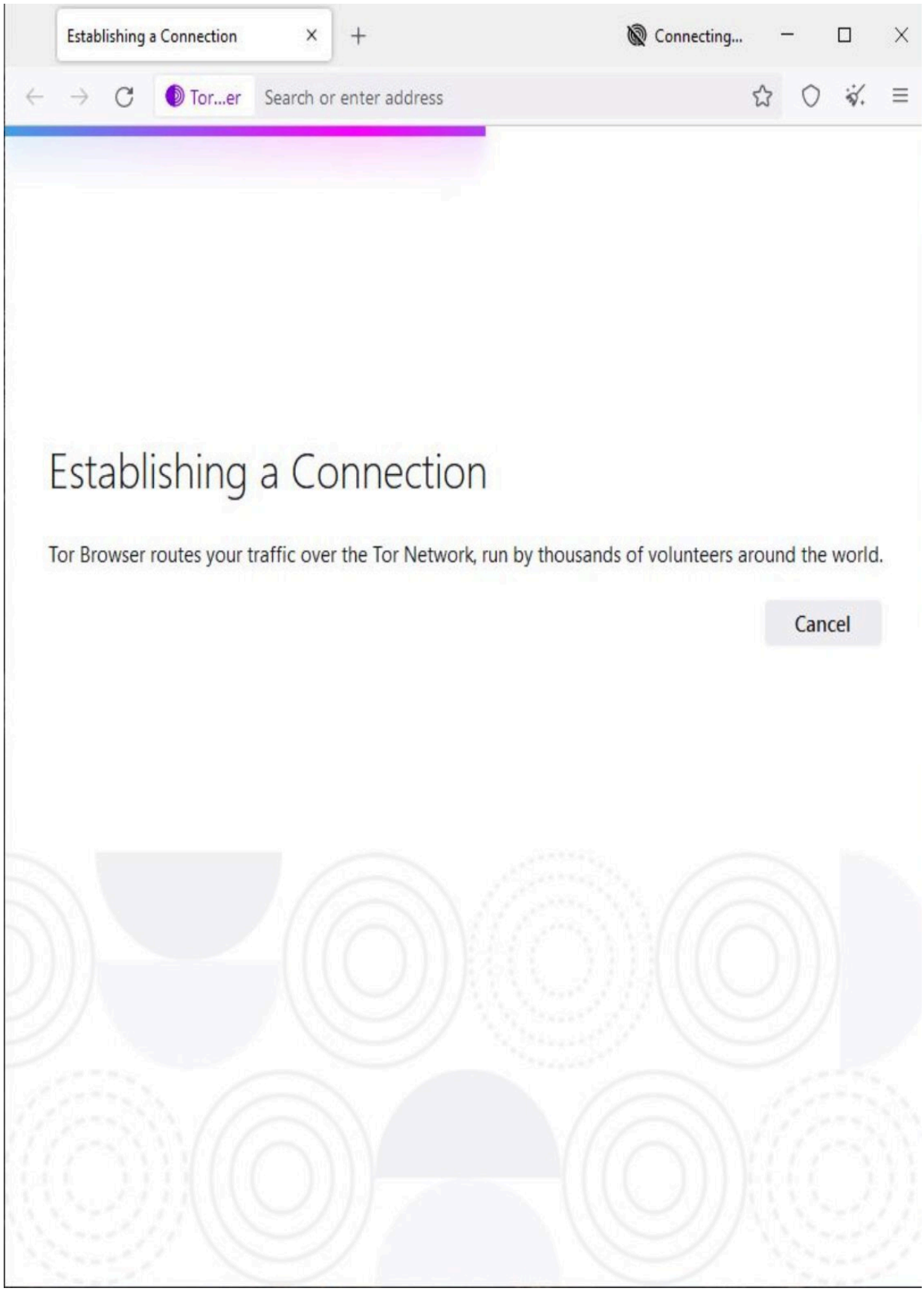

ONION BROWSER
DuckDuckGo
New York Times
BBC
ProPublica
Freedom of the Press Foundation
Deutsche Welle
Learn more about Onion Browser
Donate to Onion Browser
Subscribe to Tor Newsletter

USARE TOR SU WINDOWS E SU LINUX

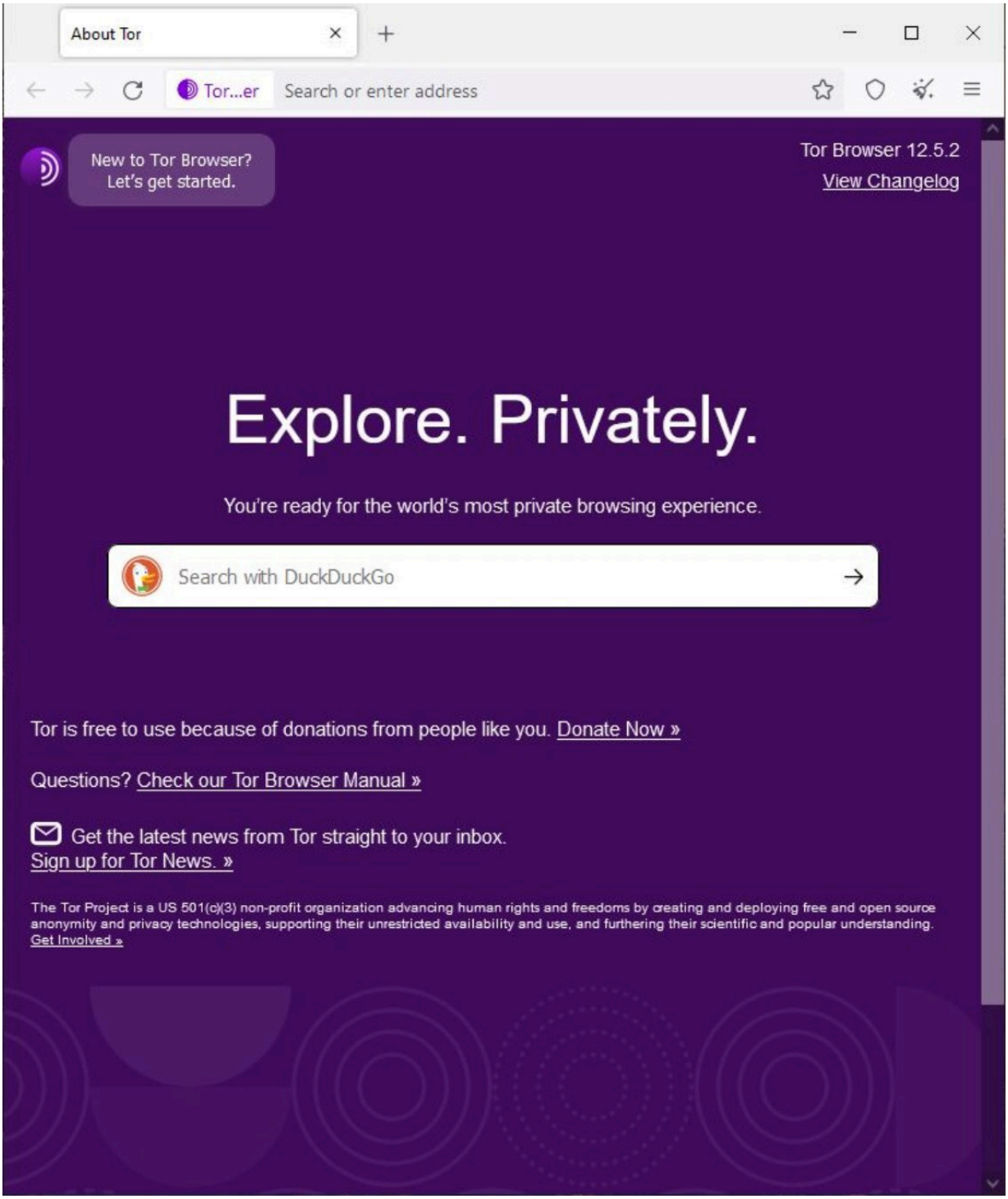
Se hai Windows fai doppio click sull'icona di TOR Browser, oppure avvialo dal menu start. Se hai Linux fai doppio click sull'icona di TOR Browser (se ce l'hai sul Desktop), oppure dall'equivalente del menu start di Windows (su Ubuntu si chiama "Dash").


Connect to Tor
Not connected
Tor...er
Search or enter address
Connect to Tor
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Always connect automatically
Configure Connection...
Connect

Fai click sul tasto "Connect". Il browser si collegherà alla rete TOR.


Establishing a Connection
Connecting...
Tor...er
Search or enter address
Establishing a Connection
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Cancel

Non appena la connessione sarà stabilita, potrai navigare sul web di superficie o sul dark web, semplicemente cercando qualcosa o inserendo un indirizzo sulla barra in alto.


About Tor
Tor...er
Search or enter address
New to Tor Browser?
Let's get started.
Tor Browser 12.5.2
View Changelog
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Tor is free to use because of donations from people like you. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox.
Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.
Get Involved »

MA COS'È QUESTO DUCKDUCKGO?

Se hai cercato qualcosa con TOR Browser, avrai notato che i risultati non ti sono stati restituiti da Google ma da un altro motore di ricerca con l'icona di un'anatra: si chiama DuckDuckGo.

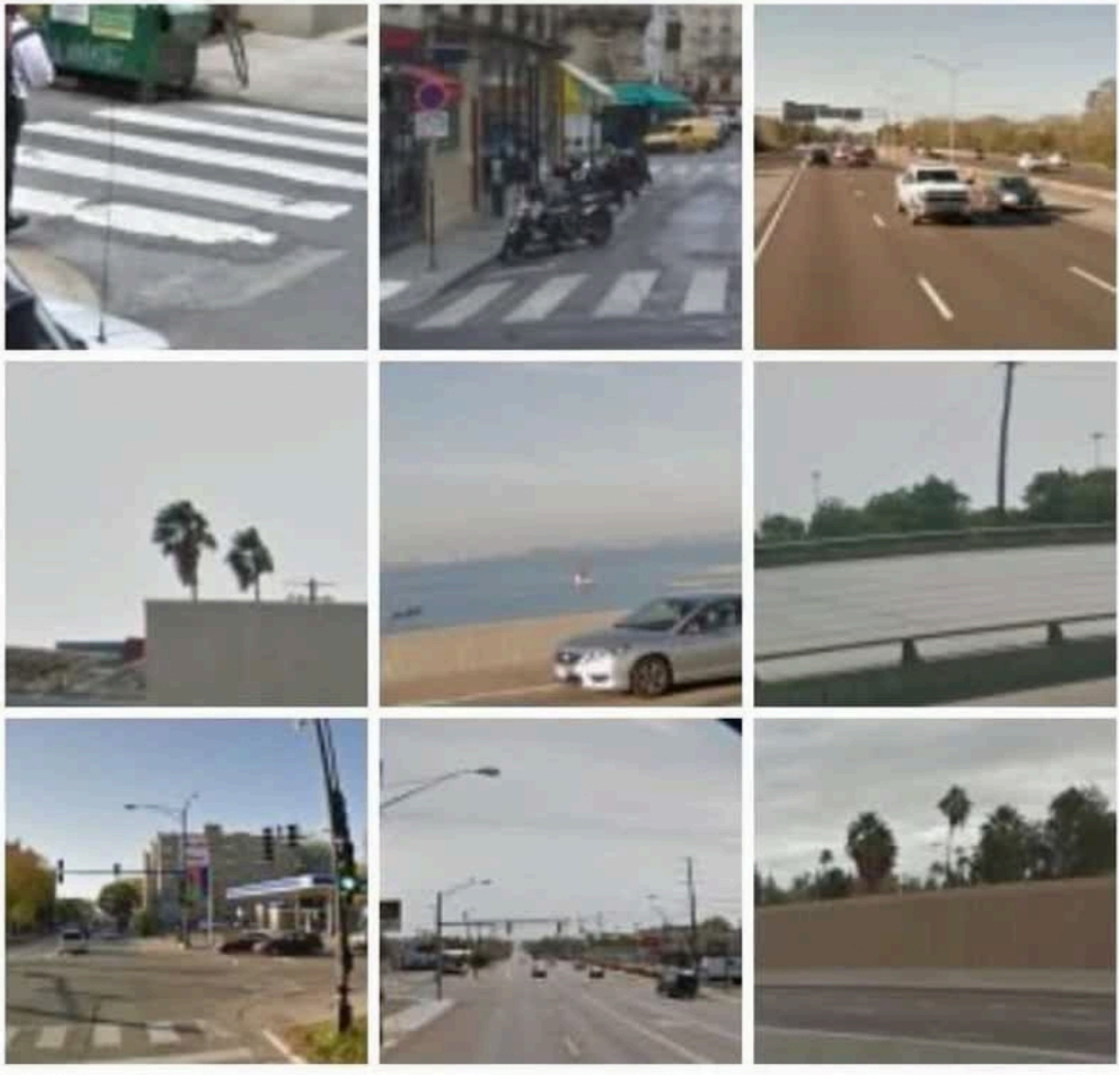
Se digiti **google.com** nella barra dell'indirizzo di TOR Browser ti comparirà un avviso di connessione non sicura, come se google non supportasse HTTPS. In realtà Google supporta benissimo questo protocollo ma se ti collegherai attraverso TOR a Google la cosa non piacerà per nulla.

Puoi anche proseguire nella navigazione ma ti comparirà un altro avviso: "abbiamo rilevato un'attività inusuale da questo indirizzo IP ..." eccetera. Ti verranno mostrati sicuramente dei CAPTCHA (quelle odiose rotture di scatole che ti chiedono di identificare moto, auto e strisce pedonali).

Select all images with

crosswalks

Click verify once there are none left.



VERIFY

Tralasciando le motivazioni tecniche sul perché questo avvenga, il concetto di fondo da capire è questo: Google non dà la minima importanza alla tua privacy. Farà di tutto pur di tracciarti, perché l'anonimato non gli piace.

Fortunatamente abbiamo a disposizione DuckDuckGo, un motore di ricerca alternativo a Google che rispetta la privacy della persone:

- Non conserva i log di accesso
- Non memorizza gli indirizzi IP dei visitatori
- Non ricorda quello che viene cercato
- Non traccia gli utenti: non "collega" al browser o al dispositivo i dati delle ricerche effettuate

DuckDuckGo è disponibile anche sul web di superficie. Non è necessario attivare TOR per accedervi.

COS'È TAILS?

Ti consiglio fortemente di usare TOR Browser nel modo che ti ho descritto sopra (ovvero installando l'app sul tuo cellulare o il programma sul tuo PC) solo per visitare i siti del web di superficie ma non quelli del dark web. I motivi sono essenzialmente due.

Primo: usare TOR Browser in questo modo non evita il tracciamento del sistema operativo. Ti ricordi di cosa si tratta? Windows, Linux, iOS ed Android mantengono informazioni dettagliate sulla tua attività scrivendole nei file di log. E questi sono difficili da cancellare.

Ciò vuol dire che se il dispositivo col quale ti sei connesso a TOR viene rubato o sequestrato, chi ne viene in possesso può esaminare i file di log per ricostruire tutta la tua attività, mandando a quel paese la negazione verosimile.

Secondo (e fondamentale) motivo: il dark web è pieno zeppo di virus. I virus (o "malware") sono programmi come tutti gli altri, solo che hanno scopi malevoli.

Quindi usare TOR Browser sotto Windows (il sistema operativo che vanta il maggior numero di malware al mondo) non è esattamente una buona idea. E non lo è nemmeno usarlo con Android.

E non credere che i dispositivi Apple siano immuni da virus: non lo sono affatto (anche se la possibilità di beccare un malware per macOS o iOS è statisticamente molto bassa).

Ma chi si prende la briga di disseminare il dark web di malware, e perché? Ci sono diversi motivi per farlo.

Le forze dell'ordine potrebbero approntare un finto sito pedopornografico, per cercare di rintracciare i pedofili. Stessa cosa potrebbero fare gli hacker etici per lo stesso scopo.

In molti altri casi, dei semplici malintenzionati potrebbero approntare un sito "esca" (di qualunque genere) col solo scopo di installarti un virus che resterà buono buono nel tuo computer, tentando di rubarti il numero della tua carta di credito appena possibile.

Come si può fare ad evitare questi due problemi? Come già accennato, la cosa migliore è utilizzare un sistema operativo "amnesico". TAILS è uno di essi ed è stato concepito apposta per essere usato con TOR.

TAILS è una sigla: significa "The Amnesic Incognito Live System", "sistema operativo live amnesico per la navigazione in incognito". Per capire bene come funziona devo accennare un minimo a come funziona internamente un elaboratore.

Ogni computer (cellulari compresi) ha al suo interno tre componenti fondamentali:

- La CPU: è la parte che esegue i programmi

- La memoria principale: è la parte che memorizza i dati in modo permanente. Nei computer si chiama "hard disk" oppure "SSD"

- La RAM: è anche lei una memoria, solo che è temporanea. Appena spegni il dispositivo, tutti i dati che contiene vengono persi

A cosa serve la RAM? Quando fai doppio click sull'icona di un programma, esso viene prelevato dalla memoria principale e messo in RAM, perché la RAM è molto più veloce. Il computer, in tal modo, riesce ad eseguire il programma in modo più rapido.

E lo stesso vale per il sistema operativo: Android è "installato" (risiede) dentro alla memoria principale del telefono. IOS è installato dentro alla memoria dell'iPhone. Windows, Linux e macOS sono installati dentro all'hard disk o alla SSD del computer.

Un sistema operativo "live" non tocca i dati dell'hard disk o della SSD: viene eseguito su un'unità esterna, tipicamente una chiavetta USB. Linux Ubuntu, ad esempio, dà la possibilità di essere eseguito in modalità "live" per dare modo all'utente di provarlo.

I sistemi operativi live tracciano comunque l'attività dell'utente mantenendo i file di log: solo che essi sono salvati sulla chiavetta esterna invece che sulla memoria principale.

TAILS è un sistema live che viene solo "avviato" (fatto partire) da una chiavetta USB ma che poi viene eseguito interamente nella RAM, senza toccare né i file contenuti nella memoria principale del computer né quelli contenuti nella chiavetta USB.

Ecco perché è "amnesico": quando spegni il computer o stacchi la chiavetta, tutto quello che hai fatto viene subito dimenticato, garantendo la negazione verosimile. Inoltre un malware qualunque avrebbe vita molto breve, visto che infetterebbe un sistema che al prossimo riavvio ripartirà "da zero".

TAILS non è disponibile per i cellulari o per i tablet. Può essere usato solo con un PC o con un Mac.

Ti consiglio vivamente di accedere al dark web esclusivamente attraverso TAILS e di non utilizzare un cellulare o un tablet. A parte la negazione plausibile ed il pericolo malware, usare un PC è molto più pratico che utilizzare un dispositivo con schermo piccolo. Come vedrai, i siti del dark web non sono ottimizzati per i cellulari.

COME SI INSTALLA TAILS?

Per installare TAILS, è sufficiente andare qui:

https://tails.net/

Poi dovrai premere su "Install TAILS", scegliere il sistema operativo che vuoi usare per installarlo (tra Windows, macOS e Linux) e seguire le istruzioni passo-passo. Queste sono disponibili anche in italiano ma sono tradotte male o solo parzialmente.

Ti riporterò la procedura per Windows, dettagliandola un po' meglio e spiegandoti anche alcuni concetti che ti aiuteranno a capire per bene quello che stai facendo. Le procedure per macOS e Linux sono concettualmente analoghe. Ti assicuro che se capisci quella per Windows non avrai nessuna difficoltà con gli altri sistemi.

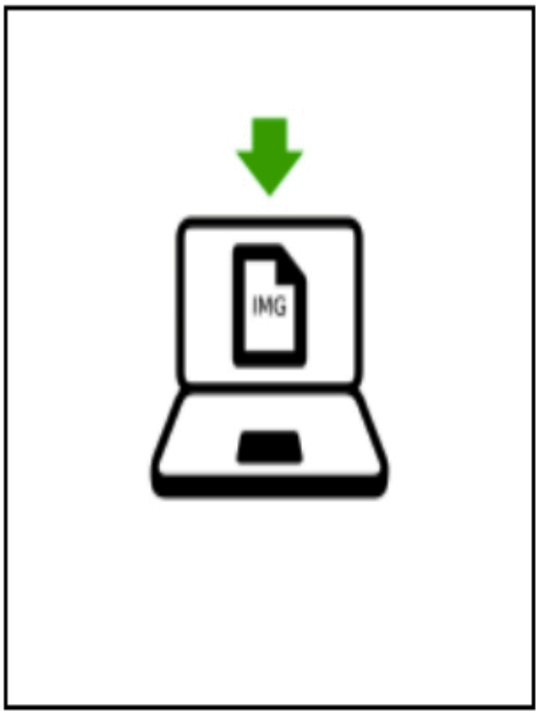
Sostanzialmente, lo scopo della procedura guidata è creare una chiavetta USB avviabile che contenga TAILS. Intanto partiamo con l'elenco di quello di cui avrai bisogno:

- Una chiavetta USB da almeno 8 GB. Tutto il contenuto della chiavetta verrà distrutto, quindi occhio a quella che scegli

- Un PC con Windows 7 o superiore ed almeno 2 GB di memoria RAM

Passaggio 1: scarica TAILS premendo sul tasto verde.

1/9 Download Tails



Download Tails 5.16.1 USB image (1.3 GB)

or download using BitTorrent

Passaggio 2: verifica che il file scaricato sia quello autentico.

A cosa serve questo passaggio? Se un attaccante volesse spiare chiunque utilizzi TAILS, potrebbe facilmente approntare un sito con una grafica identica a quella del sito ufficiale ed indurre i malcapitati a scaricare una versione modificata di TAILS, fatta apposta per spiare gli utenti.

La contromisura consiste nel verificare che il file sia "autentico". È possibile farlo usando un espediente matematico simile alla crittografia che si chiama "PGP Signature" (vuol dire "firma PGP").

Funziona più o meno così:

- Un programma "speciale" genera una "firma" a partire da un file
- Questa "firma" è una sequenza di caratteri incomprensibili
- Ogni file genera una firma diversa: non possono esistere due file che abbiano firma uguale, a meno che essi non siano assolutamente identici
- I programmatori di TAILS pubblicano la firma PGP del vero TAILS
- Per accertarsi di essere in possesso del TAILS "autentico" non devi fare altro che generare la firma del file che hai scaricato e confrontarla con quella "ufficiale"

Questo sistema non viene utilizzato solo da TAILS ma anche per accertarsi che i file scaricati da internet non siano "rovinati" (può succedere se hai una connessione instabile o se ci sono stati errori durante il trasferimento).

Ci sono due modi per verificare la firma di TAILS: scaricare il programma gratuito "OpenPGP" oppure premere direttamente sul tasto "Select your download..." sotto alla sezione "Verify your download".

3/9 Verify your download

Verify your download to make sure that it is safe and was not corrupted during download.

Select your download...

Passaggio 3: Scaricare ed installare BalenaEtcher.

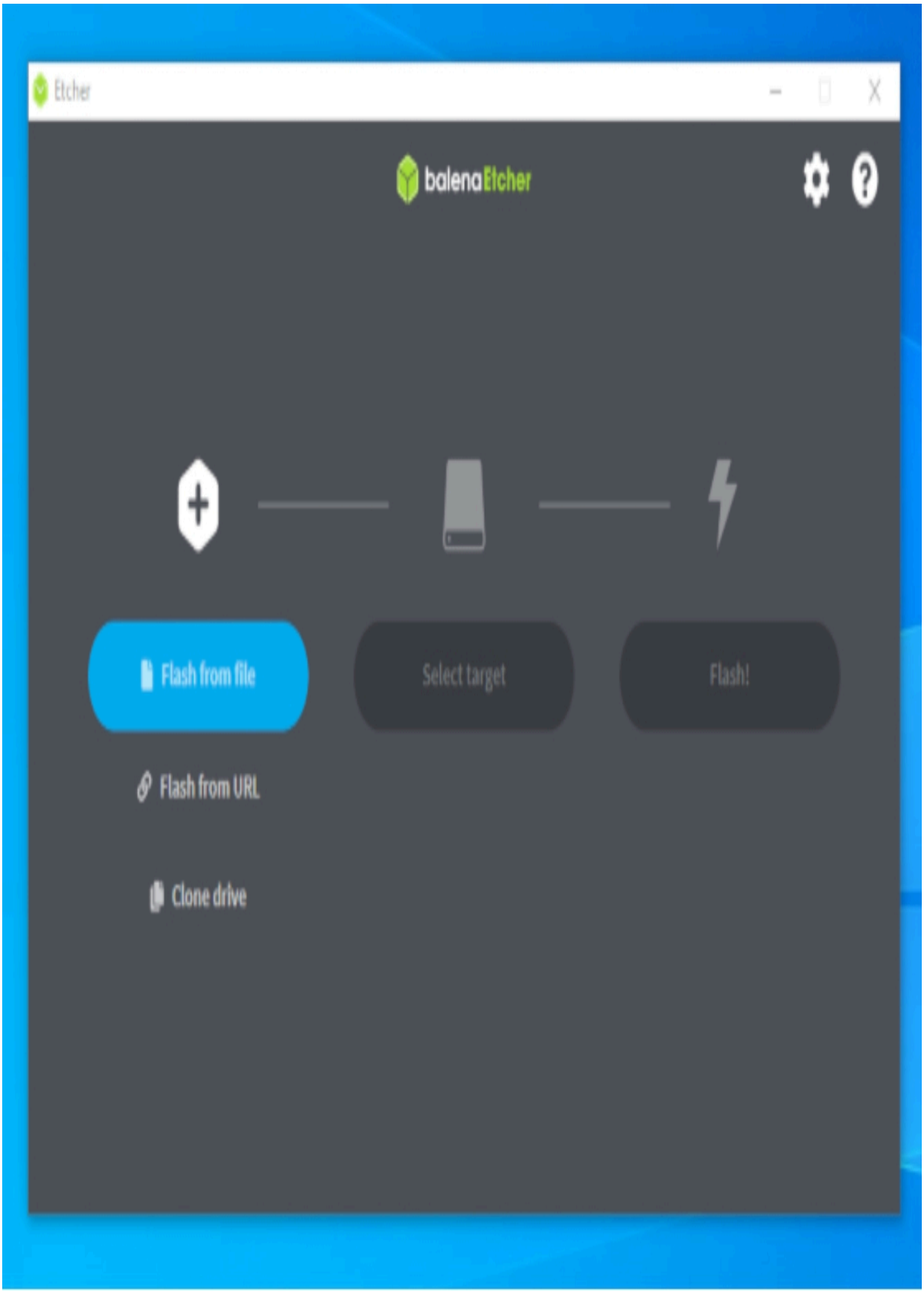
Questo programma dal nome singolare è uno dei molti in grado di creare chiavette USB avviabili. Premi sul tasto verde "Download BalenaEtcher for Windows", aspetta che il file si scarichi e facci sopra doppio click.

4/9 Download *balenaEtcher*

1. Click on the following button to download *balenaEtcher*:

Download balenaEtcher for Windows

Windows potrebbe mostrarti una finestra in cui ti chiede il permesso di eseguire il file appena scaricato. È una misura di sicurezza. I virus sono programmi come tutti gli altri, ricordi? Windows non sa se BalenaEtcher è attendibile. Tu però si, per cui acconsenti tranquillamente all'esecuzione del programma. Ti comparirà una schermata molto intuitiva.


Etcher
balenaEtcher
Flash from file
Select target
Flash!
Flash from URL
Clone drive

Non devi fare altro che premere a sinistra sull'icona con il "+" e selezionare "l'origine" (il file che vuoi scrivere sulla chiavetta USB, nel nostro caso TAILS).

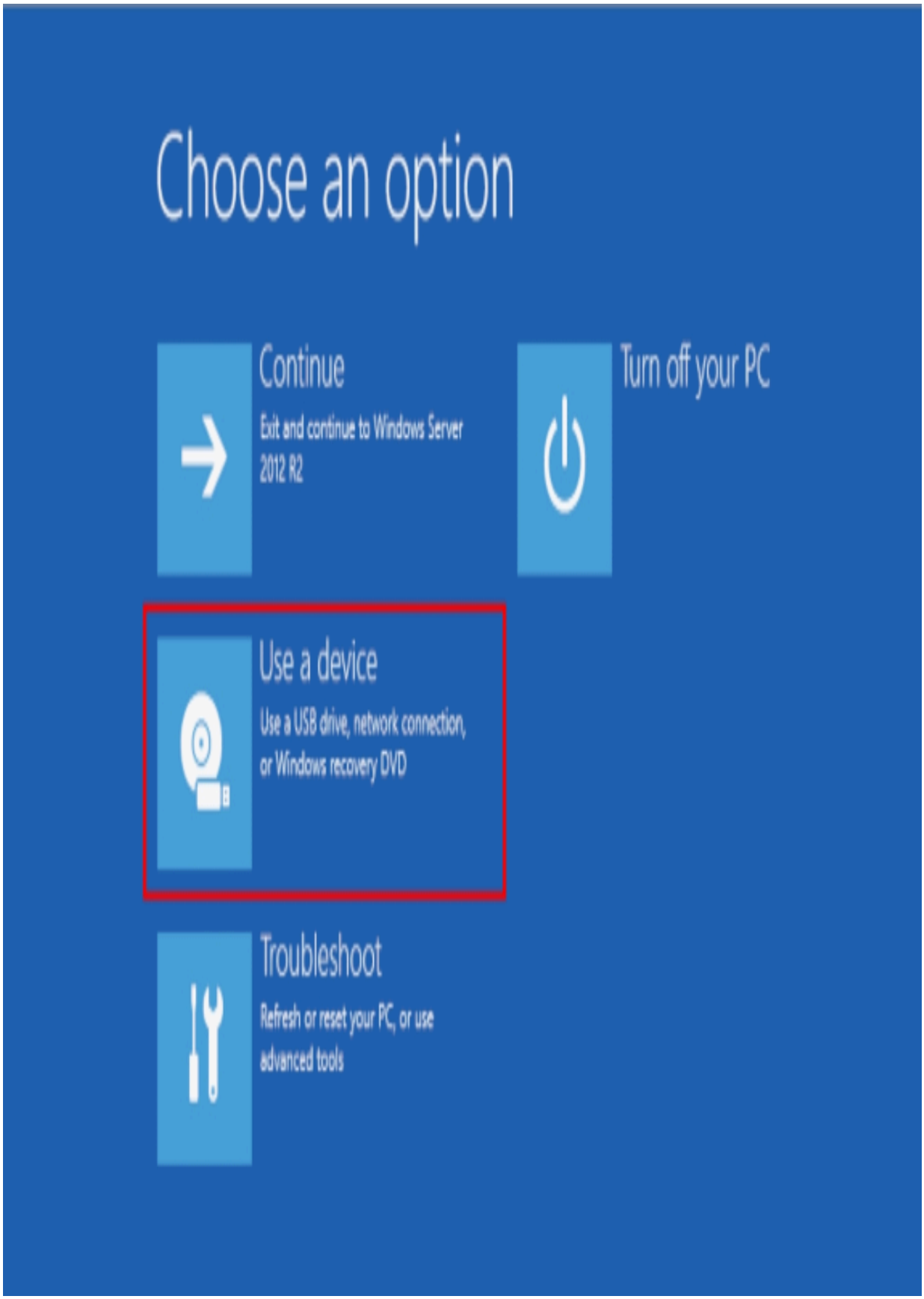
Dopo averlo fatto, dovrai inserire la chiavetta USB "di destinazione" (quella sul quale vuoi scrivere TAILS) e selezionarla.

Sei pronto: premi a destra sul tasto "Flash" (che nel frattempo sarà diventato blu) e attendi qualche minuto.

COME AVVIARE TAILS

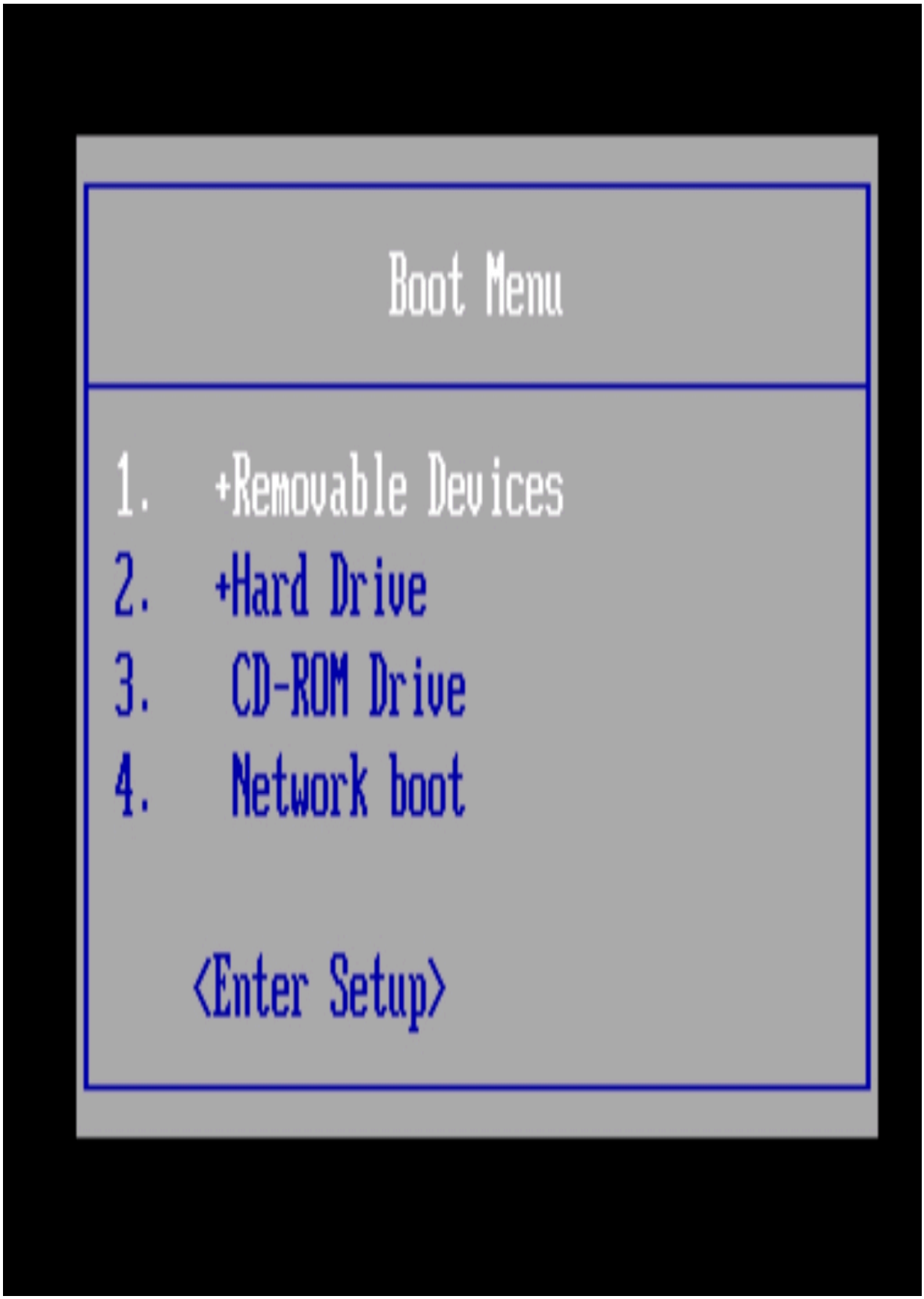
È pronta la chiavetta USB? Benissimo. Ora dovrai riavviare il tuo PC e dirgli di caricare il sistema operativo dalla chiavetta USB e non dalla memoria principale (hard disk o SSD che sia). Sotto Windows c'è un modo semplicissimo per farlo:

- Premi il menu start (quello in basso a sinistra col logo di Windows)
- Premi e tieni premuto il tasto "shift" (Quello lungo con la freccia in alto. Ce ne sono sempre due sulla tastiera: uno più o meno in basso a sinistra e l'altro più o meno in basso a destra)
- Mentre continui a tenere premuto il tasto shift, premi sul tasto "arresta" e seleziona la voce "riavvia"
- Invece di riavviarsi subito, il computer ti mostrerà una schermata blu con delle opzioni.


Choose an option
Continue
Exit and continue to Windows Server 2012 R2
Turn off your PC
Use a device
Use a USB drive, network connection, or Windows recovery DVD
Troubleshoot
Refresh or reset your PC, or use advanced tools

- Premi su "usa un dispositivo", poi premi su "Boot Menu" (vuol dire "menu di avvio")

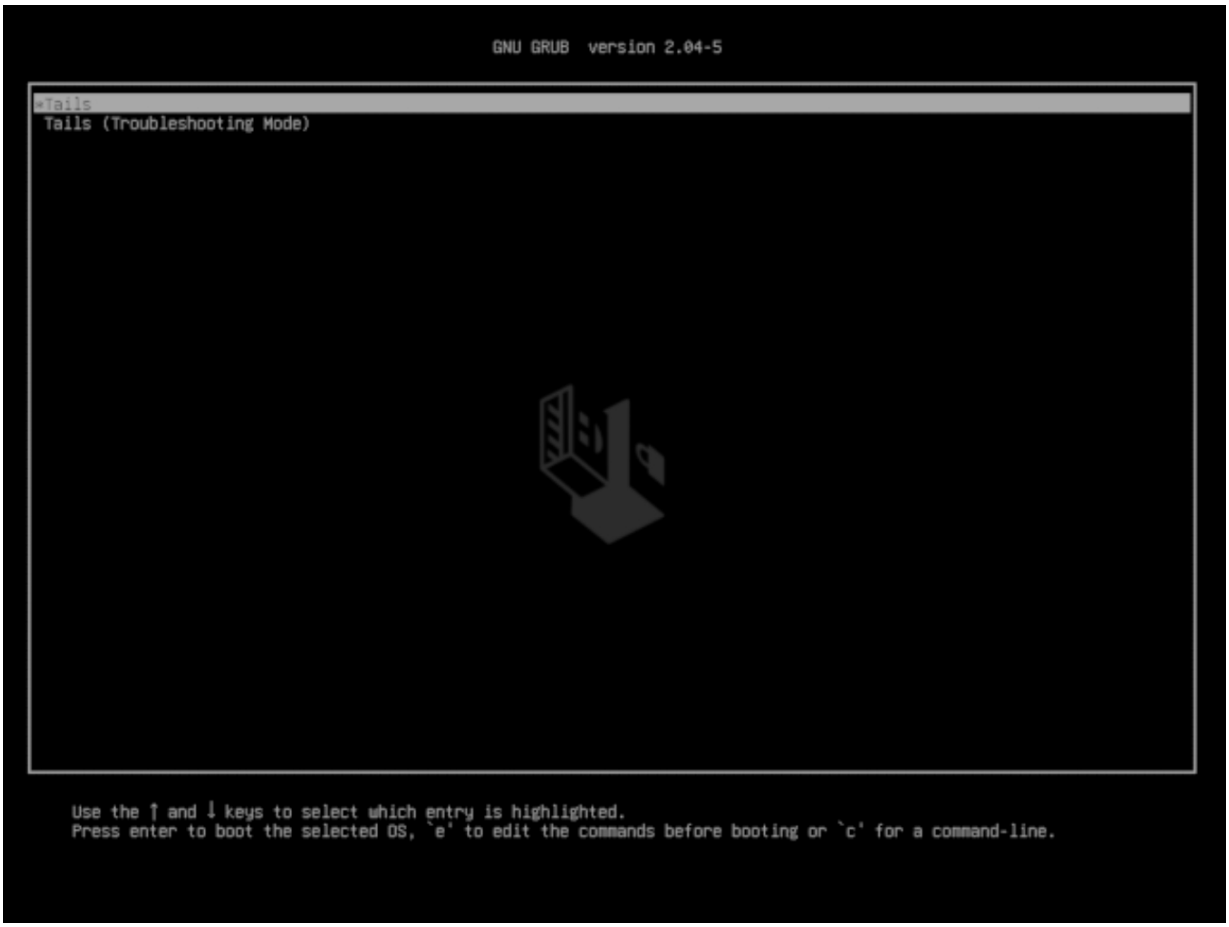
- Il "Boot menu" è una schermata in cui puoi scegliere da quale dispositivo avviare il tuo computer


Boot Menu
1. +Removable Devices
2. +Hard Drive
3. CD-ROM Drive
4. Network boot
<Enter Setup>

Se la schermata di Windows non compare oppure non hai Windows, dovrai far comparire il boot menu in un altro modo. È sempre possibile farlo, su qualunque PC. Basta premere un tasto durante la fase di avvio.

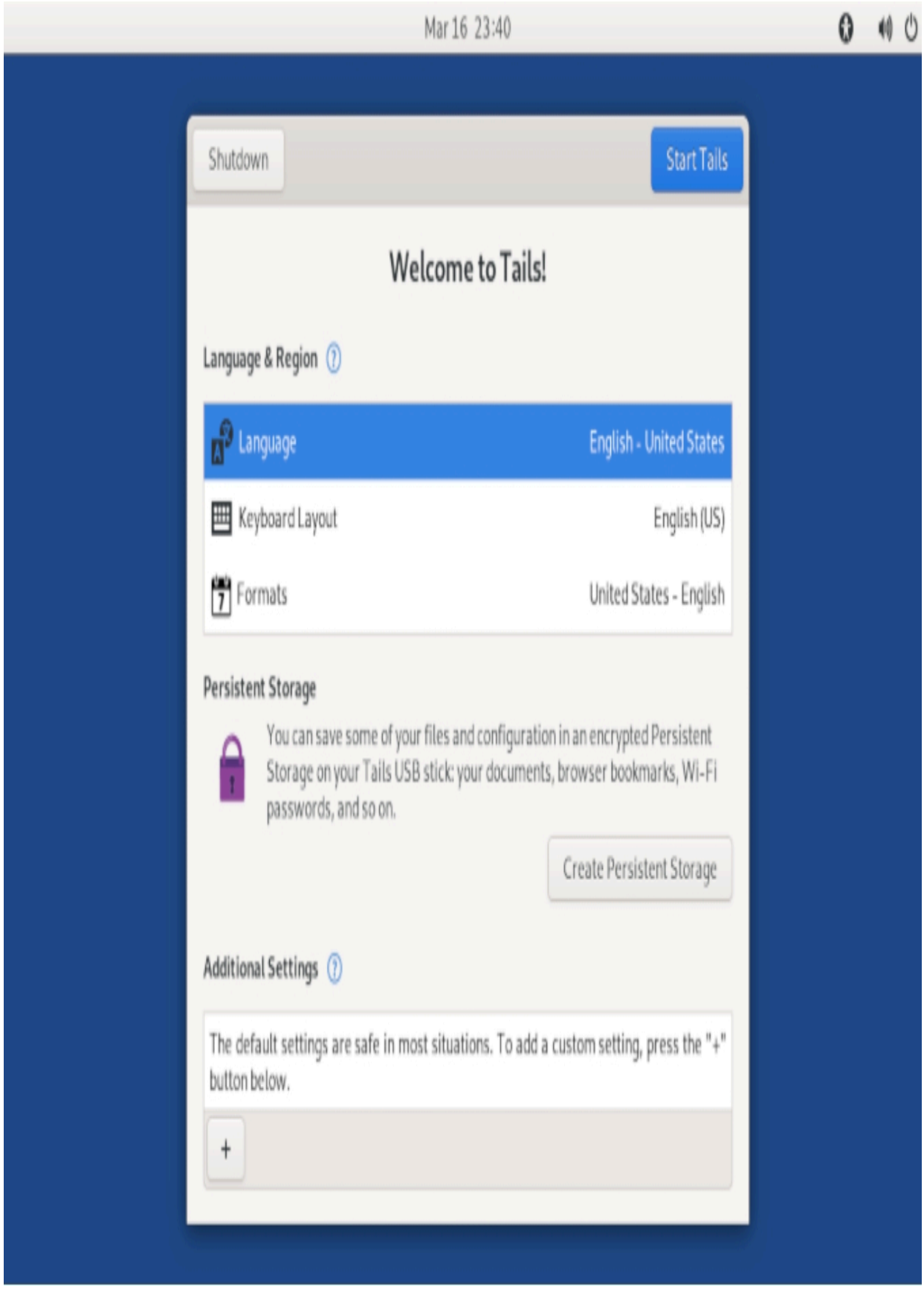
Il tasto da premere varia a seconda del modello del tuo PC. Tipicamente è il tasto CANC oppure uno dei tasti funzione (F1, F2 ... eccetera). Per scoprirlo, cerca su Google "come avviare boot menu PC ASUS N551JK" (o qualunque altro modello di computer tu abbia).

Scegli la tua chiavetta USB dal boot menu e premi invio. Ti comparirà una schermata nera con delle opzioni. Puoi alternativamente premere invio o attendere 4 secondi, trascorsi i quali TAILS si avvierà automaticamente.


GNU GRUB version 2.04-5
*Tails
Tails (Troubleshooting Mode)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

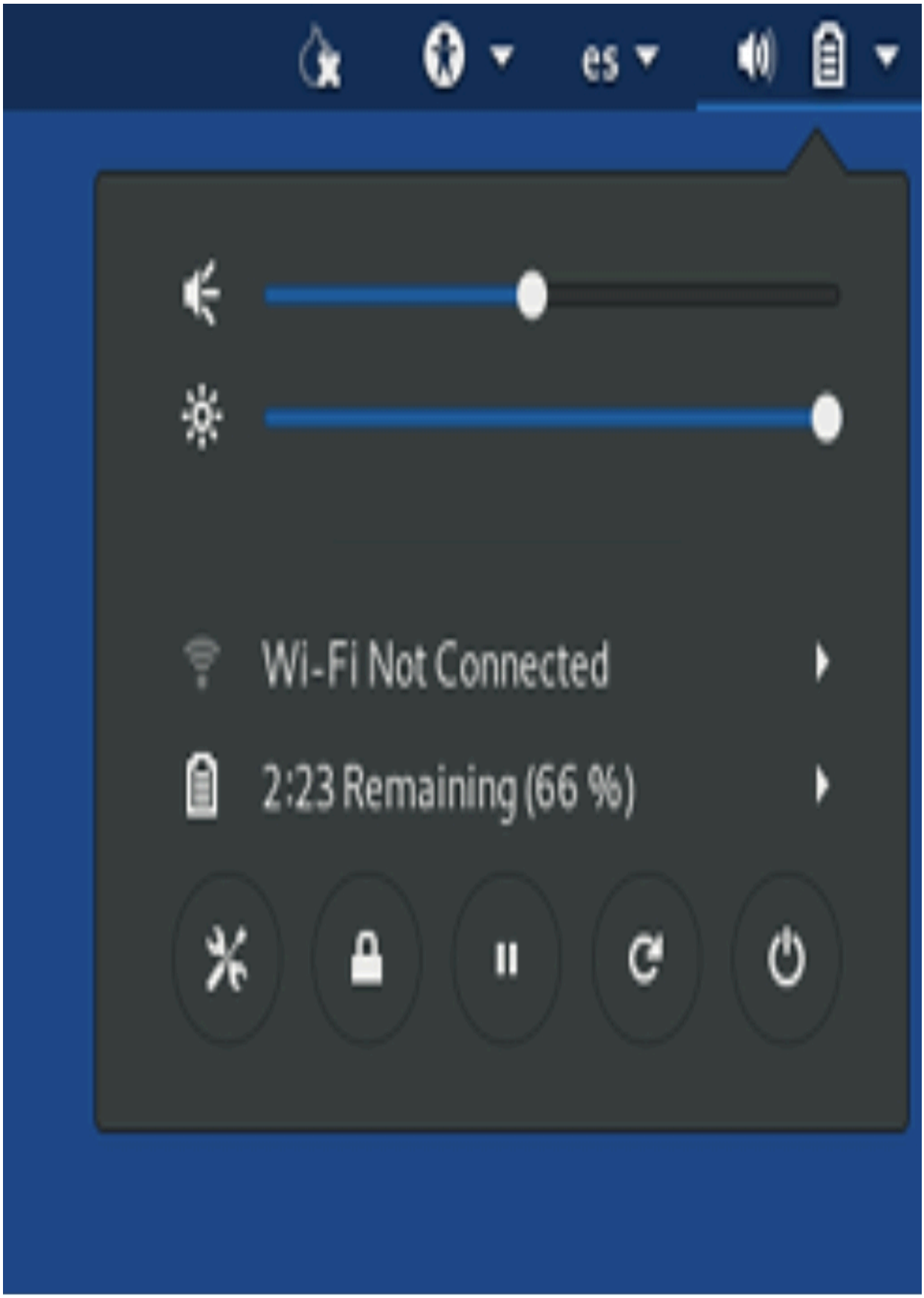
COME SI USA TAILS?

TAILS ci metterà un po' ad avviarsi: le chiavette USB sono sempre più lente delle memorie principali dei computer. Quando avrà finito, la prima schermata che ti comparirà sarà quella in cui selezionare la lingua e la configurazione della tastiera.


Mar 16 23:40
Shutdown
Start Tails
Welcome to Tails!
Language & Region
Language
English - United States
Keyboard Layout
English (US)
Formats
United States - English
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Additional Settings
The default settings are safe in most situations. To add a custom setting, press the "+" button below.
+

Dopo qualche altro secondo, ti comparirà il "desktop" (la schermata principale) di TAILS. La prima cosa che dovrai fare sarà scegliere il tuo collegamento ad internet:

- Vai sull'angolo in alto a destra
- Premi su "WiFi Not Connected"
- Scegli una rete WiFi ed inserisci la password


es
Wi-Fi Not Connected
2:23 Remaining (66 %)

Dovrai inserire la password ad ogni avvio, perché TAILS è amnesico, ricordi? Non ricorda nulla di quello che fai. Non è pensato per essere comodo ma per renderti anonimo.

In alternativa alla WIFi puoi anche collegarti con un cavo di rete al tuo modem router, come faresti normalmente con Windows.

Dopo esserti connesso, comparirà l'assistente alla connessione. TAILS forza la connessione attraverso TOR, per questo all'inzio ti chiederà come vuoi connetterti a questa rete. Puoi scegliere la connessione automatica o l'opzione per nascondere la connessione a TOR.

Tor Connection

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.

- ○ **Connect to Tor automatically (easier)**

  We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

- ◉ **Hide to my local network that I'm connecting to Tor (safer)**

  You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

Learn more about how Tails connects to Tor

Connect to Tor

Scegliendo la prima opzione non dovrai fare nient'altro. Se selezioni la seconda opzione ti comparirà una schermata che ti chiede se vuoi configurare un TOR Bridge (è un espediente per nascondere al tuo provider il fatto che ti stai collegando con TOR, ricordi?).

Tor Connection

Configure a Tor bridge

Bridges are secret Tor relays. Use a bridge as your first Tor relay if accessing Tor is blocked from where you are.

Learn more about Tor bridges

- [ ] Use a default bridge

- [x] Ask for a Tor bridge by email

  Send an empty email to `bridges@torproject.org` from a Gmail or Riseup email address with your phone and scan the QR code that is attached to the automatic reply.

  Scan QR code

- [ ] Enter a bridge that you already know

  Bridge obfs4 ...

To save your bridge, create a Persistent Storage on your Tails USB stick.

Back

Connect to Tor

Ti chiedo scusa per la pessima qualità dell'immagine di sopra. Si, è esattamente quello che sembra: una foto del mio monitor fatta col cellulare. Purtroppo catturare le schermate di TAILS è un'operazione un po' difficile.

Tornando al TOR Bridge, dovrai mandare un' email all'indirizzo **bridges@torproject.org.** Puoi anche lasciare vuoti l'oggetto ed il corpo del messaggio). Riceverai dopo qualche secondo una risposta automatica con un elenco di almeno 3 bridge TOR.

Ora dovresti, in teoria, inserire a mano la stringa che hai ricevuto, il che non è affatto semplice visto che è piena zeppa di caratteri "strani". Fortunatamente, se stai usando un PC con una webcam puoi premere sul tasto "Scan QR Code" ed inquadrare il codice QR che compare in fondo al messaggio mail.

bridges@torproject.org 12:57

A: [redacted]

[no subject]

[This is an automated email.]

Here is your bridge:

If it doesn't work, you can try this other bridge:

Fatto? Benissimo: Ora sei connesso con TOR. Puoi visitare il web di superficie in tutta sicurezza e collegarti ai siti del dark web. Non dovrai fare altro che premere sul tasto "Start Tor Browser".

Prima di proseguire però ti darò alcune indicazioni di sicurezza e ti spiegherò come fare a capire se stai navigando sul web di superficie o sul dark web.

CONSIGLI PER LA NAVIGAZIONE ANONIMA

Ecco una lista di cosa da fare e da non fare quando vuoi navigare in modo anonimo.

- Accertati che la versione di TAILS che stai usando sia l'ultima. Le versioni meno recenti potrebbero avere delle vulnerabilità sfruttabili per mettere a repentaglio la tua sicurezza ed il tuo anonimato. In ogni caso, non appena ti collegherai ad internet con TAILS sarà il sistema operativo stesso ad avvisarti della disponibilità di un eventuale aggiornamento. Se ricevi questo avviso, spegni il computer e ripeti la procedura di creazione della chiavetta TAILS

- Se un sito non usa HTTPS, non visitarlo

- Non usare Google né Bing. Usa solo DuckDuckGo

- Se scarichi un file qualunque dal dark web, aprilo solo dentro TAILS e solo se sei disconnesso da internet

- Non usare un client torrent via TOR. Per chi non lo sapesse, i "torrent" sono un sistema di trasferimento diretto di file da altri computer piuttosto che da server dedicati (si chiama "peer-to-peer"). Se vuoi scaricare file con bittorrent mascherando il tuo indirizzo IP, usa una VPN al posto di TOR

- Non scaricare file video. Evita anche di visualizzarli dentro al browser. La rete TOR è molto lenta, non è adatta allo streaming ("trasmissione") di video. Probabilmente non riusciresti a caricarlo ed inoltre

rallenteresti l'intera rete TOR. Per lo stesso motivo, evita di scaricare qualunque altro tipo di file molto pesante

- So che sembra folle ma non mettere la finestra di TOR Browser a tutto schermo. Altrimenti il sito al quale ti colleghi avrà un'informazione in più su di te (la dimensione dello schermo del computer che stai utilizzando)

- Non installare plugin (programmi aggiuntivi) dentro a TOR Browser e non cambiare nessuna preferenza. Se lo farai, diventerai più riconoscibile. In particolare, non cambiare le impostazioni di lingua e paese. Facendolo comunicheresti ai siti il fatto di provenire da un certo paese o di parlare una certa lingua

- Lascia Javascript disattivato. Spiegato in modo molto approssimativo, Javascript è un linguaggio che viene usato per rendere le pagine web più belle e funzionali, offrendo la possibilità di aggiungere animazioni o di tenere traccia dell'attività dei visitatori. Può essere usato anche per rilevare il tuo vero indirizzo IP, anche se sei connesso attraverso TOR

- Se ti iscrivi ad un servizio del dark web, non usare una casella mail che hai precedentemente usato sul web di superficie. Inoltre non usare caselle come Gmail, Libero, Virgilio o Outlook. Devi usarne una anonima (più avanti ti suggerirò quale)

- Se ti iscrivi ad un servizio attraverso TOR, non usare quel servizio senza prima collegarti a TOR

- Non scegliere username e password che contengano informazioni che potrebbero essere usate per rintracciarti. Se nella vita reale gli amici ti chiamano "aspide" (tanto per fare un esempio a caso), non usare questo nomignolo come nickname o password. Se il tuo gatto si chiama "spritz", vale la stessa regola

- Non consultare siti con contenuti illegali. Specialmente se si tratta di siti perdopornografici. Stanne alla larga il più possibile. Non accedere mai a siti di questo tipo, nemmeno per curiosità, nemmeno per sbaglio! Oltre ad essere una cosa illegale ed immorale, potresti incappare in un

"sito esca" creato apposta per rintracciare i pedofili. L'ultima cosa che vuoi è dover rendere conto delle tue azioni a causa di una inutile bravata

- Non usare TOR per accedere a siti che possiedono i tuoi dati personali. Ad esempio: se acquisti da Amazon non collegarti ad Amazon usando TOR

Potrei continuare all'infinito con questa lista di raccomandazioni. L'argomento della privacy e dell'anonimato su internet, come vedi, è vasto e complesso.

Seguire le raccomandazioni che ti ho elencato ti darà sicuramente un alto grado di anonimato. Ricorda sempre però che l'anonimato al 100% su internet non esiste. O quasi: dipende molto da quello che fai, e non solo in termini di contromisure tecniche. Intendo proprio in termini di azioni che compi.

Ripeto: se fai qualcosa di illegale, essere rintracciati è spesso solo questione di quanto tempo e denaro si è disposti ad investire.

DISTINGUERE IL WEB DI SUPERFICIE DAL DARK WEB

La distinzione tra dark web e web "normale" è una cosa sul quale moltissime persone si confondono. Molti installano TOR Browser o TAILS, si connettono a TOR e pensano di essere entrati del dark web. Ed infatti, parecchi da quel punto in poi non sanno cosa fare. Ora ti chiarirò meglio le idee. Prima però ripassiamo un attimo qualche concetto fondamentale:

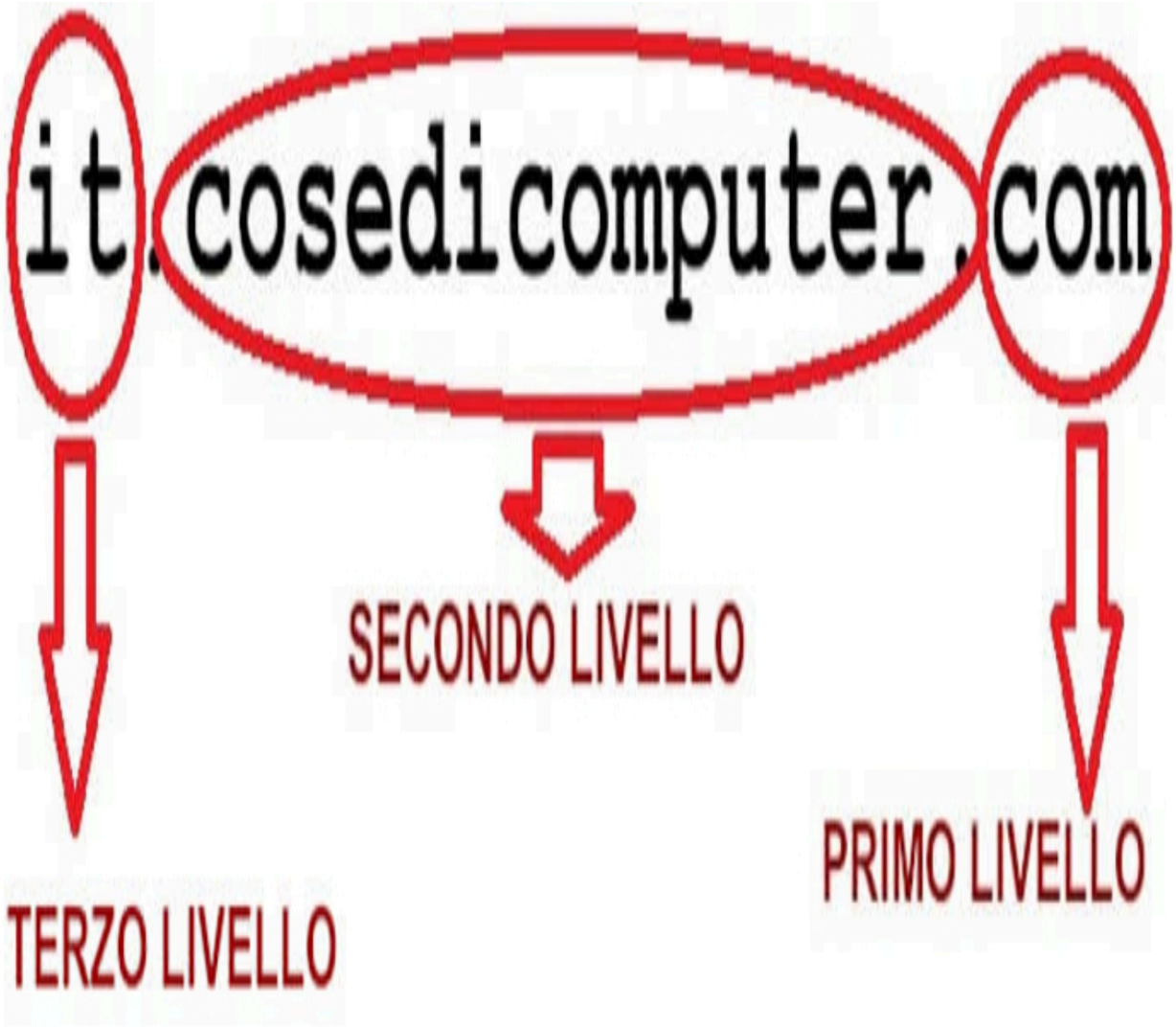
- TOR è una darknet
- Le darknet sono reti "sovrapposte" ad internet, concepite per fornirti un altissimo grado di privacy ed anonimato
- Collegandoti ad una darknet puoi navigare sul web di superficie (cioè sui siti "normali") in modo anonimo
- Collegarsi ad una darknet è l'unico modo per accedere al dark web
- Il dark web è una parte minuscola di tutto il web, che contiene siti pensati per essere consultati in modo anonimo

Tutto chiaro? Bene. Ora collegati a TOR ed apri il TOR Browser. Ti consiglio fortemente di usare TAILS ma se non vuoi, non puoi o ritieni di non aver bisogno della protezione offerta da questo sistema, fa lo stesso: da questo momento in poi tutte le istruzioni che troverai valgono per qualunque versione di TOR browser tu stia utilizzando.

La distinzione tra web di superficie e dark web è in realtà molto semplice: cambia solamente la struttura degli indirizzi dei siti.

I siti web di superficie hanno tutti un nome a dominio. Sono dei nomi che identificano in maniera univoca un sito internet. Ad esempio: **cosedicomputer.com**.

I nomi a dominio sono divisi in “livelli” che si contano partendo da destra ed andando verso sinistra. Ad esempio, in cosedicomputer.com il “primo livello” è “com” ed il secondo livello è “cosedicomputer”. Opzionalmente, i siti possono avere anche dei terzi livelli. Il più comune di essi è “www”, una sigla che sta per “World Wide Web” e che significa “rete a livello mondiale”. La stringa "www" viene messa quasi sempre come terzo livello per pura convenzione.



I nomi a dominio di primo livello non possono essere decisi arbitrariamente: sono stabiliti da un ente regolatore che si chiama IANA. Chiunque può registrare un nome a dominio. Può scegliere arbitrariamente il secondo livello ma non il primo: dovrà selezionarlo da una lista.

I nomi a dominio che appartengono al dark web hanno tutti un unico primo livello:

.onion

Un tipico indirizzo del dark web potrebbe essere ad esempio questo:

s4k4ceiapwwgg7sph7jjppqkvwwqtyd.onion

Ovvero: lettere incomprensibili, seguite da un puntino, seguito dal primo livello "onion". I nomi a dominio del dark web sono scritti così perché devono essere anonimi e difficili da ricordare, al contrario di quelli del web di superficie che sono pubblici e possibilmente facili da ricordare.

Quindi, riassumendo, non dovrai fare altro che aprire TOR browser e tenere sotto controllo la barra dell'indirizzo. Se leggi una cosa simile a questa:

https://**s4k4ceiapwwvwwqtyd.onion**/qualcosa

Allora sei nel dark web. Se invece leggi una cosa come questa:

https://**www.cosedicomputer.com**/qualcosa

Vuol dire che sei nel web di superficie ma stai navigando in modo anonimo grazie a TOR.

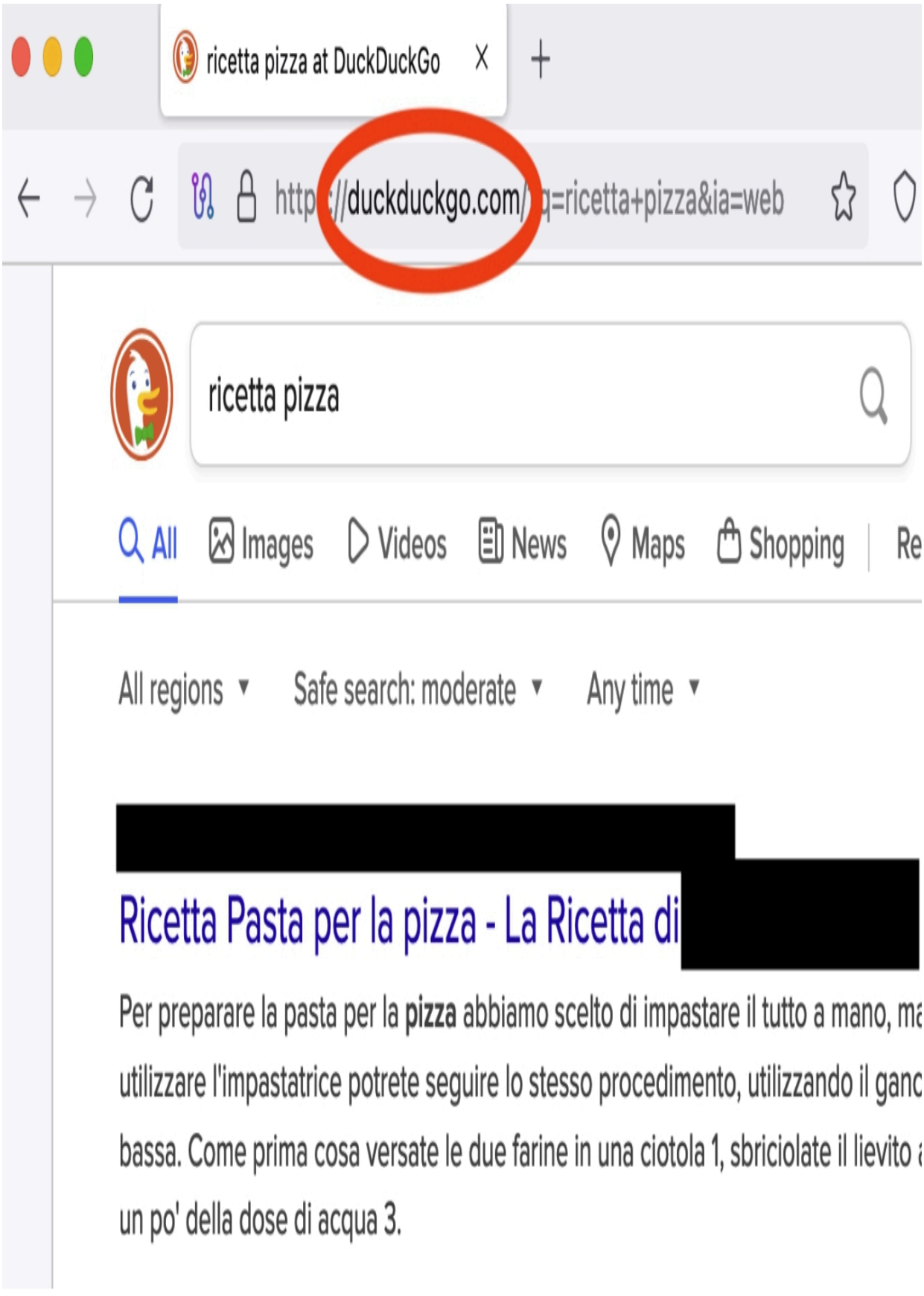
PRIMI PASSI NEL DARK WEB

Benvenuto all'inferno!

Scherzi a parte, il dark web viene dipinto così dai giornalisti per acchiappare i click ma in realtà è solo una porzione di internet visitabile in modo anonimo, che in parte contiene anche materiale scabroso o illegale.

Chi apre per la prima volta TOR browser non sa mai cosa fare. Sul web di superficie siamo abituati ad inserire qualche parola ed a premere un tasto. Sul dark web, invece, le cose non funzionano in questo modo.

Come ho già accennato, esistono dei motori di ricerca per il dark web ma non funzionano bene come Google, perché il dark web è nato apposta per non essere indicizzato. Pertanto, se inserisci delle parole dentro TOR browser e premi invio otterrai questo risultato:


ricetta pizza at DuckDuckGo
http://duckduckgo.com/?q=ricetta+pizza&ia=web
ricetta pizza
All
Images
Videos
News
Maps
Shopping
Re
All regions
Safe search: moderate
Any time
[redacted]
Ricetta Pasta per la pizza - La Ricetta di [redacted]
Per preparare la pasta per la pizza abbiamo scelto di impastare il tutto a mano, ma
utilizzare l'impastatrice potrete seguire lo stesso procedimento, utilizzando il ganc
bassa. Come prima cosa versate le due farine in una ciotola 1, sbriciolate il lievito a
un po' della dose di acqua 3.

Ti si aprirà la pagina dei risultati di ricerca di DuckDuckGo. Dai un'occhiata all'indirizzo dentro alla barra del browser: è nel formato

https://**duckduckgo.com**/qualcosa

Stai visitando un sito web di superficie e non un sito del dark web (si vede dal nome a dominio). In pratica, ecco cosa è successo:

- Hai digitato delle parole nella barra di ricerca
- Quelle parole sono state passate a DuckDuckGo, che è un motore di ricerca anonimo alternativo a Google
- DuckDuckGo ti ha restituito alcune pagine del web di superficie che contengono le parole che hai cercato
- Il tutto è stato terribilmente lento

Hai cercato qualcosa come avresti fatto abitualmente, solo che lo hai fatto passando attraverso la rete TOR. Quindi sei perfettamente anonimo, nel senso che DuckDuckGo non sa chi tu sia. E la connessione è stata lenta perché ha dovuto attraversare tutti gli strati della "cipolla".

I siti del dark web sono molto più brutti di quelli di superficie perché "pesano" di meno e non usano javascript. Contengono pochissime immagini e lo stile grafico è spesso completamente assente. Non sono fatti per essere belli ma per essere veloci a caricarsi. Per i siti web, di norma, vale questa regola: più brutto = più veloce.

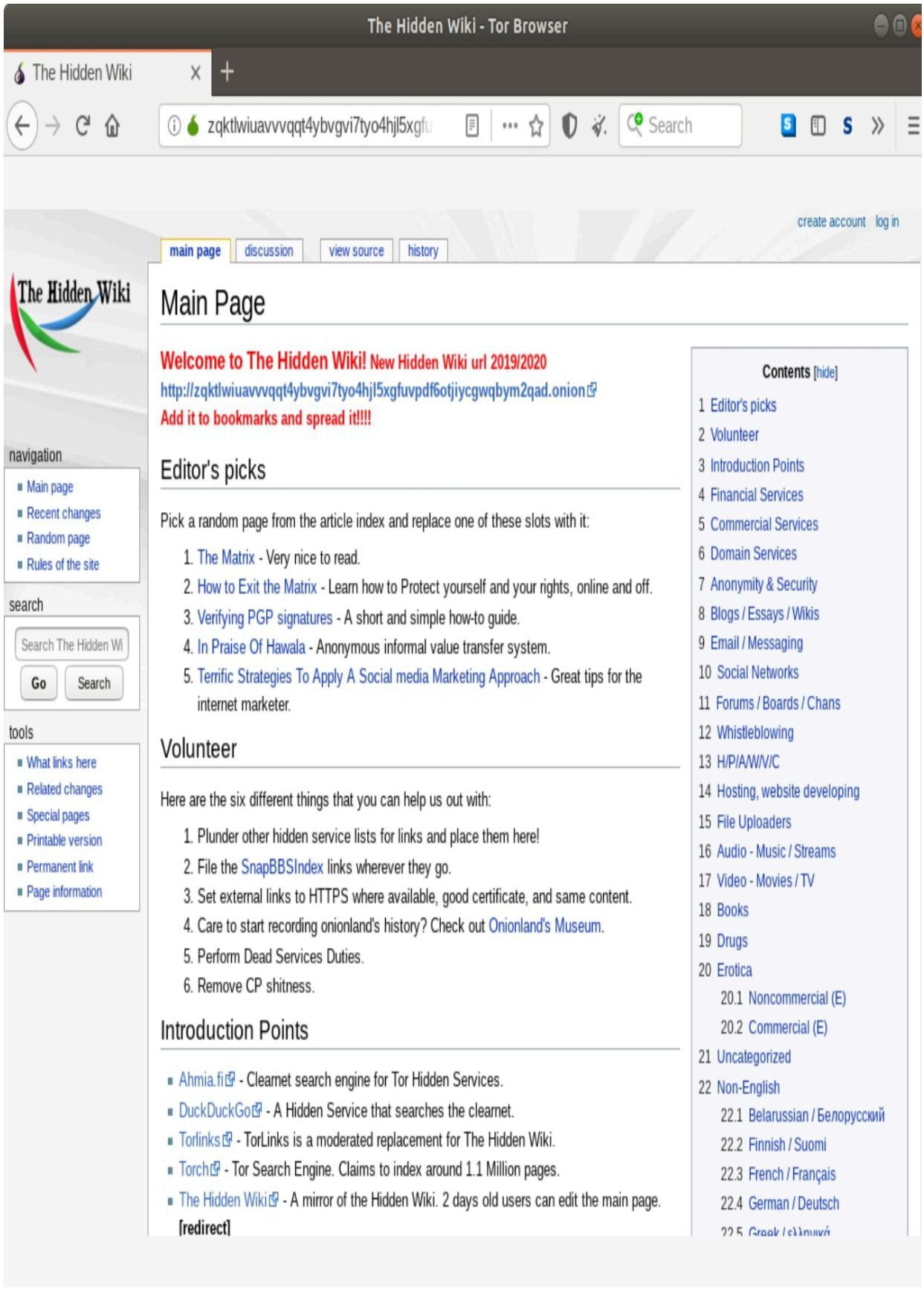
Per "entrare nel vivo" del dark web devi visitare un sito che abbia un indirizzo che finisce per .onion. Come trovarli? Tipicamente, il primo passo consiste nel visitare un "entry point" (punto di ingresso). Sono siti web che contengono link ad altri siti del dark web.

L'entry point più noto si chiama "hidden wiki" ("wiki nascosta"). Il termine "wiki" indica un sito che può essere modificato da chiunque. Wikipedia è senza dubbio il più noto sito di questa categoria.

Se cerchi le parole "hidden wiki address" ti verranno fuori molti risultati. Quello che devi trovare lì in mezzo è l'indirizzo onion della hidden wiki "originale", che potrebbe non essere facile da scovare.

Questo perché la hidden wiki ha spesso ospitato anche link a siti con materiale pedopornografico. Pertanto la prima versione è stata hackerata, per poi venire ripristinata ed attaccata di nuovo, e più di una volta. Ormai se ne trovano in giro tantissime versioni, molte delle quali sono "censurate" (non contengono collegamenti a materiale illegale).

Non so indicarti una procedura esatta per trovare la hidden wiki. Cerca un po' sul web di superficie finché non trovi un indirizzo valido. Saprai di essere sulla pagina corretta se ti comparirà una schermata simile a questa:


The Hidden Wiki - Tor Browser
The Hidden Wiki
zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfu
Search
create account
log in
main page
discussion
view source
history
The Hidden Wiki
Main Page
Welcome to The Hidden Wiki! New Hidden Wiki url 2019/2020
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Add it to bookmarks and spread it!!!!
navigation
Main page
Recent changes
Random page
Rules of the site
search
Search The Hidden Wi
Go
Search
tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information
Editor's picks
Pick a random page from the article index and replace one of these slots with it:
1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.
Volunteer
Here are the six different things that you can help us out with:
1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Perform Dead Services Duties.
6. Remove CP shitness.
Introduction Points
Ahmia.fi - Clearnet search engine for Tor Hidden Services.
DuckDuckGo - A Hidden Service that searches the clearnet.
Torlinks - TorLinks is a moderated replacement for The Hidden Wiki.
Torch - Tor Search Engine. Claims to index around 1.1 Million pages.
The Hidden Wiki - A mirror of the Hidden Wiki. 2 days old users can edit the main page.
[redirect]
Contents [hide]
1 Editor's picks
2 Volunteer
3 Introduction Points
4 Financial Services
5 Commercial Services
6 Domain Services
7 Anonymity & Security
8 Blogs / Essays / Wikis
9 Email / Messaging
10 Social Networks
11 Forums / Boards / Chans
12 Whistleblowing
13 H/P/A/W/V/C
14 Hosting, website developing
15 File Uploaders
16 Audio - Music / Streams
17 Video - Movies / TV
18 Books
19 Drugs
20 Erotica
20.1 Noncommercial (E)
20.2 Commercial (E)
21 Uncategorized
22 Non-English
22.1 Belarussian / Белорусский
22.2 Finnish / Suomi
22.3 French / Français
22.4 German / Deutsch

Nel momento in cui scrivo, comunque, l'indirizzo della hidden wiki è questo:

zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

Attenzione: alcune hidden wiki non sono quelle "originali" ma delle "trappole" messe lì da forze dell'ordine o hacker etici. Quindi fai attenzione a dove clicchi. In particolare, evita tutti i siti con la dicitura CP: significa "Child Porn", ovvero "pedopornografia".

Esistono tantissimi altri entry point. Nel momento in cui scrivo, ad esempio, esiste questo sito:

https://thehiddenwiki.org/

Hidden Wiki – TheHidden

The darknet guide – The Hidden Wiki

HIDDEN WIKI MORE DEEP WEB ARTICLES

2021
06.21

Hidden Wiki

Category: / Tags: no tag / Add Comment

To browse .onion deep web links, install Tor bro

http://torproject.org/

If you are looking for the best dark web sites, the Hidden Wiki

New .onion links 2021

Hidden Wiki sites

http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjp

v3

http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkha

Wiki

http://2jwcnprqbugvyi6ok2h2h7u26qc6j5wxm7feh3znlh2qu3

Hidden Wiki

È un sito di superficie che contiene link onion di vario genere.

Purtroppo non posso darti una lista precisa di entry point, perché cambiano in continuazione. Però sono abbastanza facili da scovare: la pagina che ti ho indicato sopra l'ho trovata inserendo "hidden wiki address" su DuckDuckGo.

Se non capisci l'inglese avrai qualche difficoltà: tutto (o quasi) il contenuto del dark web è scritto in questa lingua. Però non scoraggiarti: dopo un po' di tempo entrerai nella "terminologia" e riuscirai a navigare più facilmente.

Per trovare pagine interessanti sul dark web bisogna sostanzialmente rovistare un po' in giro. Esistono degli strumenti che possono aiutarti.

MOTORI DI RICERCA PER IL DARK WEB

Come già detto, non esiste un Google del dark web. Ci sono però alcuni motori di ricerca, estremamente lenti e poco precisi ma che possono comunque essere utili. Ora te li elenco ma tieni presente che gli indirizzi potrebbero cambiare da un giorno all'altro.

TORCH: è probabilmente il più "antico" motore di ricerca per il dark web. Il suo indirizzo è questo:

xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion

Ahmia.fi: un motore abbastanza decente. Lo trovi qui:

juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

Non posso fare a meno di elencare anche DuckDuckGo (già lo conosci). Ne esiste una versione onion accessibile dal dark web, che però cerca informazioni solo sul web di superficie. È sostanzialmente inutile accedervi mediante l'indirizzo onion: accedervi via TOR usando l'indirizzo

di superficie ti garantirà lo stesso il pieno anonimato visto che DuckDuckGo ha una no log policy stretta. Comunque, il suo indirizzo onion è questo:

duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

Non c'è molto altro da dire: cercare informazioni sul dark web non è facilissimo. Bisogna andare a tentativi ed aspettare un po' di tempo prima che le pagine si carichino.

Comunque non demordere: curiosando in giro troverai sicuramente dei siti molto interessanti. Intanto te ne elencherò io qualcuno nel prossimo capitolo.

SITI INTERESSANTI DEL DARK WEB

Facebook: si, esiste la versione onion di Facebook, fatta apposta per consentire l'accesso a chi abita in paesi in cui questo social network è censurato.

facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion

Propublica: un interessantissimo blog gestito da volontari di un'associazione no-profit che si occupa di giornalismo investigativo.

p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion

Securedrop: un servizio dedicato ai "whistleblowers". Sono persone che entrano in possesso di informazioni riservate e che scelgono di rivelarle per il bene pubblico. Uno dei più famosi Whistleblowers è Edward Snowden, che ha rivelato al mondo alcuni programmi illegali di sorveglianza di massa. Securedrop permette di condividere informazioni riservate in modo completamente anonimo.

sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion

Riseup: un forum gestito da attivisti contrari alla sorveglianza di massa ed agli strumenti che invadono la privacy delle persone. Fornisce gratis caselle email anonime, VPN ed altri strumenti utili.

vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion

The hidden wallet: un sito che fornisce wallet (portafogli) bitcoin completamente anonimi. Vedremo più avanti cosa sono e a cosa servono i Bitcoin.

d46a7ehxj6d6f2cf4hi3b424uzywno24c7qtnvdvwsah5qpogewoeqid.onion

Protonmail: un sito che fornisce indirizzi email gratutiti e totalmente anonimi.

protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion

The New York Times SecureDrop: la pagina SecureDrop del New York Times dedicata a chi vuole inviare in modo anonimo materiale "scottante".

protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion

Come vedi nessuno dei siti che ti ho elencato sopra è "malevolo" o "sbagliato".

Nel prossimo capitolo ti spiegherò come creare un account di posta elettronica gratuito ed anonimo.

COME CREARE UN ACCOUNT EMAIL ANONIMO

Per usare i servizi del dark web è necessario avere un indirizzo email, esattamente per come avviene coi servizi forniti dai siti web di superficie.

Per mantenere l'anonimato dovrai creare un indirizzo di posta dedicato solo ai servizi del dark web, che d'ora in poi chiameremo "indirizzo dark". Inoltre dovrai seguire delle semplici regole di sicurezza:

- Non usare il tuo indirizzo normale per registrarti a servizi del dark web
- Non usare il tuo indirizzo dark per registrarti a siti web di superficie
- Usa il tuo indirizzo dark solo attraverso TOR, mai attraverso la rete internet normale

In altre parole, per avere un buon anonimato, quando entri nel dark web devi dimenticarti completamente il web di superficie. Fai finta di essere Batman: indossa maschera e costume e ricorda le precauzioni di sicurezza che ti ho già elencato.

A titolo dimostrativo, ora ti elencherò i passaggi per creare un indirizzo dark con Protonmail. Iniziamo.

Innanzitutto apri il TOR browser, possibilmente usando TAILS. Se non usi TAILS, fai molta attenzione a restare solo ed esclusivamente all'interno del TOR browser. Fai tutto da lì dentro e non aprire altri browser

Vai sul sito onion di Protonmail. Fai molta attenzione all'indirizzo: deve terminare col primo livello .onion:

protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.**onion**

Dopo il ".onion" non deve esserci nient'altro! Alcuni siti fraudolenti hanno indirizzi che ti fanno credere di essere sul dark web, mentre invece stai navigando allegramente in superficie. Ecco un esempio:

protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.**onion.to**

Il primo livello è "to" e non "onion". Guarda sempre la barra del browser quando premi un link qualsiasi!

Ora premi su "create an account" in alto a destra.

Proton

Sign in

Create a free account

Proton is privacy for everyone

Welcome to a better internet where **privacy and freedom come first**

Mail Calendar Drive VPN Pass

Scorri in basso e premi su "Get Proton for free".

Proton Free

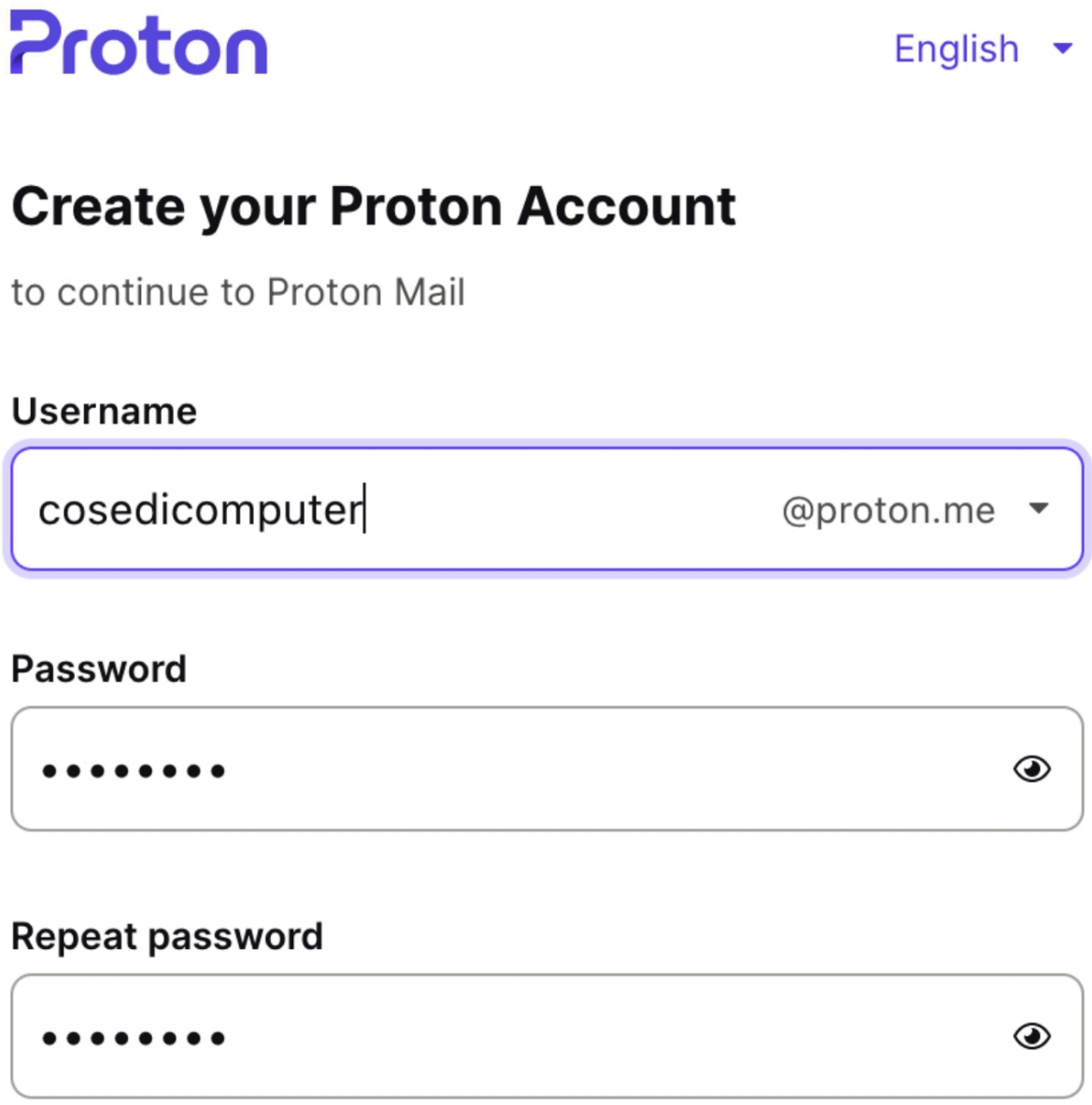
0 € /month

No credit card required

Get Proton for free

Discover features +

Inserisci un nome utente ed una password. Ricorda di non inserire come nome utente un tuo nomignolo, il nome del tuo gatto o qualunque altra informazione che ti riguardi.



Premi in basso su "create account". Quasi sicuramente Protonmail ti chiederà di inserire il tuo "vero" indirizzo email oppure un numero di cellulare, per poterti inviare un SMS con un codice di verifica.

Proton

Verification

Your email will only be used for this one-time verification.

Learn more

Email address

Get verification code

"Scusa Danilo, perché devo inserire il mio vero indirizzo o numero di telefono? L'anonimato non se ne va a quel paese?"

In realtà no. Come spiegato nella pagina di supporto di Protonmail, la conferma viene chiesta solo per evitare che vengano creati indirizzi Protonmail "usa e getta" dedicati all'invio di messaggi spam.

Puoi evitare questo passaggio comprando un piano a pagamento ma non ne vale la pena: non è un espediente per guadagnare soldi. Protonmail non salverà l'indirizzo o il numero che inserisci nella casella: memorizzerà solo un "hash crittografico", ovvero una sequenza di caratteri incomprensibili dal quale è impossibile risalire al dato vero.

Quindi procedi con fiducia. Inserisci email o telefono, apri il messaggio che riceverai subito dopo da Proton, inserisci il codice contenuto nel messaggio e premi il tasto "Verify".

Proton

Verification

Enter the verification code that was sent to

If you don't find the email in your inbox, please check your spam folder.

Verification code

Code is 6 digits without spaces

Verify

Ora ti verrà chiesto un "display name", ovvero il nome che comparirà come mittente. Ti verrà proposto il nome che hai già inserito prima, pertanto puoi anche lasciare quello.

Proton

Congratulations on choosing privacy!

To get started, choose a display name. This is what people will see when you send an email, invite them to an event, or share a file.

Display name

cosedicomputer

Next

Nella schermata successiva ti verrà chiesto di inserire un numero di telefono ed una email di recupero dell'account. Stavolta non inserire nulla ma ricorda: se perderai la password del tuo account Protonmail non sarai in grado di accedere al tuo indirizzo dark. Pertanto conservala accuratamente.

Proton

Save contact details

Save your email address or phone number to use for verification if you need to reset your account.

Recovery phone number

+1

201 555 0123

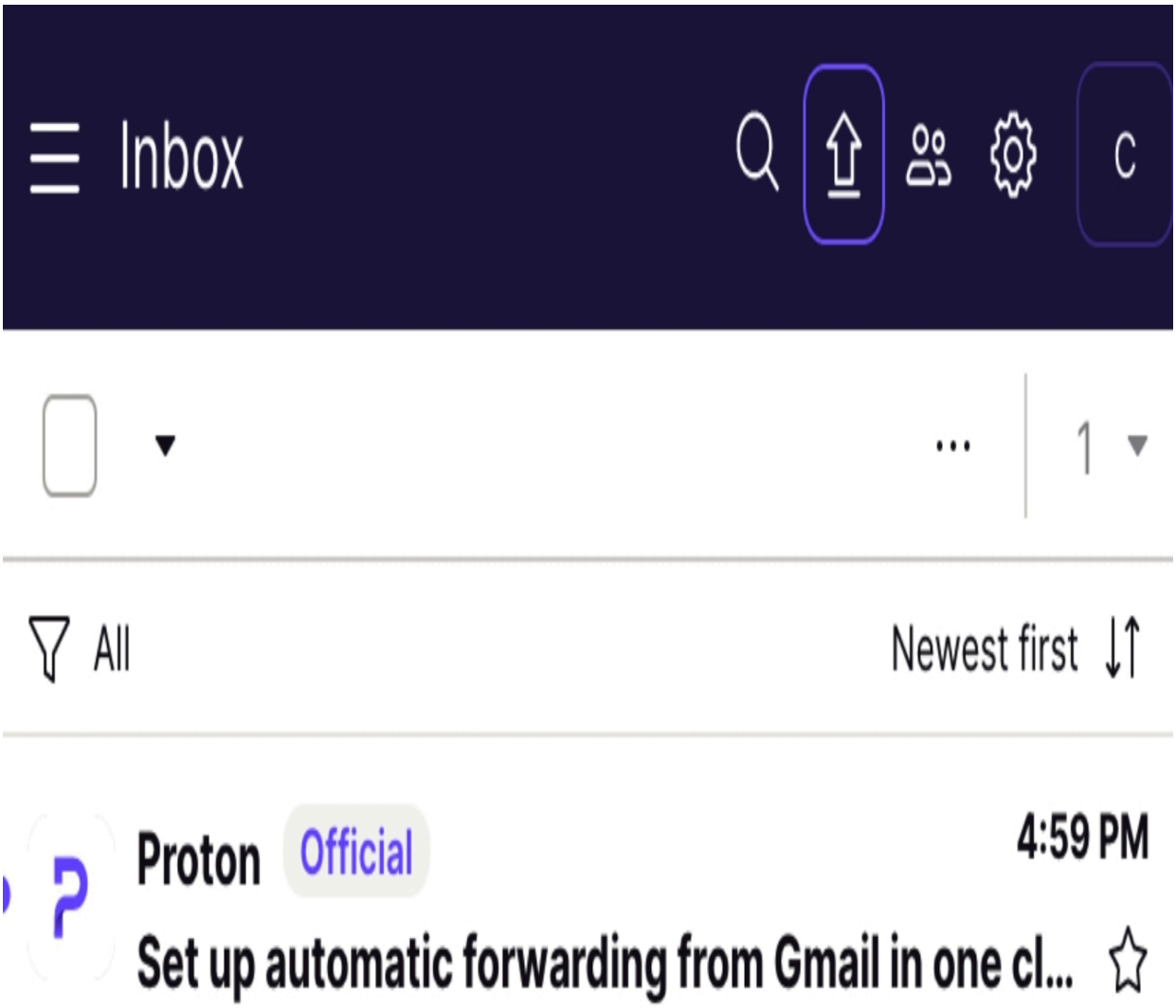
Recovery email address

Save selected

Premi su "Save Selected", poi su "Confirm". Fatto! Ecco il tuo indirizzo dark. Ricorda di non usarlo se non attraverso TOR, e soprattutto di non utilizzarlo per registrarti a siti web di superficie.

Puoi usare il tuo indirizzo dark come quello normale. Per leggere ed inviare messaggi collegati con TOR browser, poi vai sull'indirizzo onion di

Protonmail ed effettua l'accesso.


Inbox
C
1
All
Newest first
Proton
Official
4:59 PM
Set up automatic forwarding from Gmail in one cl...
Protect and simplify your email
Double your free storage to 1 GB when
you complete the following:

Ora vedremo come fare ad acquistare merce sul dark web. Prima però devo spiegarti per bene cosa sono le criptovalute.

COSA SONO LE CRIPTOVALUTE ED I BITCOIN?

Partiamo dal concetto base: cos’è una “valuta”? Può essere definita come un'unità di scambio che serve ad acquistare beni e servizi. Ogni valuta ha un nome ed un codice.

Esempio: il Dollaro Americano ha il codice USD, l’Euro ha il codice EUR. Le valute vengono emesse dagli stati sovrani attraverso le banche centrali. Ad esempio, il Dollaro statunitense viene emesso dalla Federal Reserve System. L'Euro viene emesso dalla Banca Centrale Europea (BCE).

Le banche centrali hanno il monopolio sull’emissione di una determinata moneta: nessun altro ente è autorizzato ad emetterla. Questo vuol dire che le valute tradizionali sono sostanzialmente stabili: i tassi di cambio dall’una all’altra non subiscono quasi mai oscillazioni troppo forti. Inoltre le banche centrali possono decidere di ridurre o aumentare l’emissione di nuove banconote.

Le criptovalute sono monete virtuali emesse da un programma e non da una banca centrale. Non è facile nemmeno per alcuni informatici comprendere come esse vengano emesse. La cosa fondamentale da tenere presente però è che non esiste alcuna autorità di controllo. Il loro valore è pertanto determinato unicamente dal mercato, ovvero dalla legge di domanda ed offerta. Il tasso di cambio quindi può essere estremamente variabile.

La prima e più famosa criptovaluta è senza dubbio il Bitcoin, il cui tasso di cambio può oscillare di percentuali anche considerevoli in brevissimi archi di tempo.

Esistono anche delle criptovalute stabili, il cui tasso di cambio segue quello di una valuta tradizionale. Ne è un esempio la USDC: è praticamente il dollaro americano in criptovaluta e ne segue esattamente il tasso di cambio ufficiale.

Molte figure di spicco del mondo bancario non vedono di buon occhio le criptovalute, per un motivo molto semplice: non le possono controllare. Non c'è modo per loro di regolarne l'emissione.

I Bitcoin sono stati concepiti per essere anonimi. Purtroppo però non lo sono affatto, o quasi. Per capire perché bisogna conoscere un minimo come funzionano.

COME FUNZIONANO I BITCOIN?

Se ti aspetti lo "spiegone" tecnico sul funzionamento dei Bitcoin, mi spiace deluderti. In questo capitolo ti spiegherò il funzionamento "pratico" di questa criptovaluta.

I Bitcoin, essendo virtuali, non possono essere tenuti dentro alla tasca dei pantaloni. Bisogna custodirli all'interno di app e programmi appositi chiamati "wallet" (significa "portafogli" in italiano).

I wallet Bitcoin hanno degli indirizzi che non contengono alcun tipo di dato identificativo. Ecco l'indirizzo di un wallet Bitcoin:

1Lbcfr7sAHTD9CgdQo3HTMTkV8LK4ZnX71

Come vedi è molto diverso da un IBAN, che contiene al suo interno i dati identificativi della banca ed il numero di conto corrente. Gli indirizzi infatti sono pensati per essere anonimi.

Purtroppo però non lo sono affatto. I Bitcoin usano una tecnologia che si chiama "blockchain" (catena di blocchi). Questa è pubblica e leggibile da chiunque: contiene le informazioni su tutti i trasferimenti di denaro fatti in Bitcoin a partire dal giorno in cui è stato inventato.

Immagina una stanza piena di persone che si scambiano denaro. Per rendersi anonimi indossano tutti una maschera. Può funzionare? Si e no: nessuno può dire chi sta dietro alla maschera ma tutti possono osservare il "giro" dei soldi che vengono scambiati. È una situazione di anonimato piuttosto limitata.

Se pubblichi l'indirizzo del tuo wallet Bitcoin sul tuo sito, chiunque sarà in grado di vedere la lista dei tuoi movimenti.

I Bitcoin sono anonimi solo se riesci a procurarteli in modo anonimo, li spendi in modo anonimo e non pubblichi l'indirizzo del tuo wallet in un luogo dal quale è possibile risalire alla tua identità.

Nei prossimi capitoli vedremo come procurarsi i Bitcoin e come fare a renderli anonimi.

COME CREARE UN WALLET BITCOIN

Ti consiglio caldamente di non usare un programma o un app wallet. Se vuoi restare anonimo ti conviene creare un "web wallet", cioè un wallet che puoi usare collegandoti ad un sito web. Inoltre se usi TAILS non puoi installare programmi, perché essendo un sistema amnesico dovresti poi reinstallarlo dopo ogni riavvio.

A titolo di esempio, ti riporto la procedura per creare un web wallet su "the hidden wallet" (un servizio che ho già menzionato prima).

Intanto collegati a TOR ed apri il TOR Browser. Poi vai su questo indirizzo:

d46a7ehxj6d6f2cf4hi3b424uzywno24c7qtnvdvwsah5qpogewoeqid.onion


Log in
Register
Hidden Wallet
simple and secure
Get Started

Premi sul tasto "Get Started" e ti comparirà la schermata di iscrizione. Come vedi non è richiesto l'inserimento di un indirizzo email. È una prassi diffusa per i servizi del dark web ma attenzione alla password: se la dimentichi non avrai alcun modo di recuperarla.

Create Hidden Wallet Account

Username

cosedicomputer

Set Password

••••••••

Confirm Password

••••••••

I agree to the Terms and Conditions

Create Account

Inserisci i dati e premi su "Create Account". Ti comparirà una schermata che ti mostrerà l'indirizzo del tuo wallet ed il tuo saldo attuale. Sotto c'è anche il modulo per inviare denaro a qualcuno: non dovrai fare altro che inserire l'indirizzo Bitcoin del destinatario, inserire l'importo e premere sul tasto "Send".

Your Hidden Wallet

Your Bitcoin address:

To receive Bitcoins, give the address above to the sender of the Bitcoins.

Or scan the qr code to deposit Bitcoins yourself.

You now have **0.00** bitcoins in your wallet.

To send/withdraw any of your available balance, enter the address and amount below.

Address

Address

Amount (minimum 0.005. You can send a maximum of 0.00)

Amount

Send

Facile, vero? Il problema non è gestire il wallet ma procurarsi i Bitcoin in modo anonimo.

COME PROCURARSI I BITCOIN

A meno di non farseli mandare da qualcuno che ce li ha già, non esiste altro modo di procurarsi Bitcoin se non acquistandoli. E per farlo bisogna collegarsi ad un sito di "exchange" (cambio valuta) e fornire un numero di carta di credito.

Se si vuole evitare di usare una carta intestata a se stessi è possibile comprare della carte di credito anonime prepagate (ovviamente pagandole in contanti).

Altrimenti esistono dei servizi chiamati "bitcoin mixer". Il termine è molto azzeccato perché "to mix" vuol dire "mischiare".

Sulla hidden wiki trovi diversi servizi di exchange e di Bitcoin mixing. Alcuni sono anche gratuiti. Ti risparmio i passaggi dettagliati per acquistare Bitcoin e per effettuare, se vuoi, il mixing.

Appena avrai caricato il tuo wallet Bitcoin potrai procedere ad acquistare qualcosa dal dark web.

COME ACQUISTARE SUL DARK WEB

Siamo arrivati quasi alla fine. Ora che sai come collegarti al dark web, cercare informazioni, aprire una casella email anonima e procurarti i Bitcoin, puoi procedere ad acquistare beni e servizi.

Ribadisco quanto ho già detto nei capitoli precedenti:

- L'anonimato al 100% su internet non esiste
- Se fai qualcosa di illegale, rintracciarti è spesso solo questione di quanto tempo e soldi le forze dell'ordine sono disposte ad investire

Sul dark web troverai in vendita armi, droghe, documenti falsi, medicine e dispositivi rubati. Puoi persino assoldare un hacker o un sicario. Ma se lo fai metti in conto la possibilità di essere rintracciato all'istante: le forze dell'ordine non stanno di certo a guardare e se fai qualcosa di sbagliato ne pagherai le conseguenze.

Trovi anche prodotti perfettamente legali: ad esempio libri rari, anche elettronici, oppure licenze software legittime.

Per acquistare sul dark web devi:

- Trovare un marketplace (un sito ecommerce) sul dark web
- Inserire i prodotti nel carrello
- Pagare col tuo wallet Bitcoin

Fine. Se hai già acquistato da Amazon o da eBay non hai certo bisogno del tutorial dettagliato.

CONSIDERAZIONI FINALI

Credo di essere una persona con una certa moralità e avevo dei dubbi sul divulgare informazioni che potrebbero rendere in grado le persone di fare cose pericolose o immorali.

Su internet però ci sono già migliaia di pagine con tutorial per accedere al dark web. Le informazioni contenute in questo manuale sono già di pubblico dominio. Io mi sono limitato a raccoglierle e a spiegarle in modo comprensibile.

Io non voglio che i miei lettori si mettano nei guai. In realtà vorrei che nessuno si mettesse nei guai. Purtroppo però il mondo è pieno di gente convinta che basti la scheda anonima del browser per essere "al sicuro".

Quest'opera non è dedicata ai criminali ma alle persone che non hanno dimestichezza col computer. La dedico a tutti coloro che vogliono diventare consapevoli di quanto la loro privacy sia compromessa ogni volta fanno qualcosa in rete.

Quindi, di nuovo, ti invito a non fare nulla di illegale e spero che queste pagine ti siano state utili a capire meglio gli argomenti della privacy e dell'anonimato su internet.

NON SCAPPARE VIA!

Iscriviti al mio blog andando qui:

cosedicomputer.com

Puoi anche seguirmi sul tuo social preferito: trovi i link andando sul blog e scorrendo in basso.

Fammi sapere se questo manuale è stato di tuo gradimento: contattami subito per farmi avere il tuo parere. Non esitare a farlo: la tua opinione mi sarà di grande aiuto per migliorare quello che faccio!

Se vuoi, dai anche un'occhiata agli altri miei manuali. Trovi tutto nella sezione "negozio" del mio Blog.

Grazie ancora per la tua attenzione!


INFORMATICA
DI BASE PER
PRINCIPIANTI
COMPRENDERE IN MANIERA EFFICACE I CONCETTI DI INFORMATICA PER UTILIZZARE FACILMENTE COMPUTER E SMARTPHONE
DANILO CIMINO


INFORMATICA
DI BASE PER
OVER 50
COMPRENDERE IN MANIERA EFFICACE I CONCETTI DI INFORMATICA PER UTILIZZARE FACILMENTE COMPUTER E SMARTPHONE
DANILO CIMINO