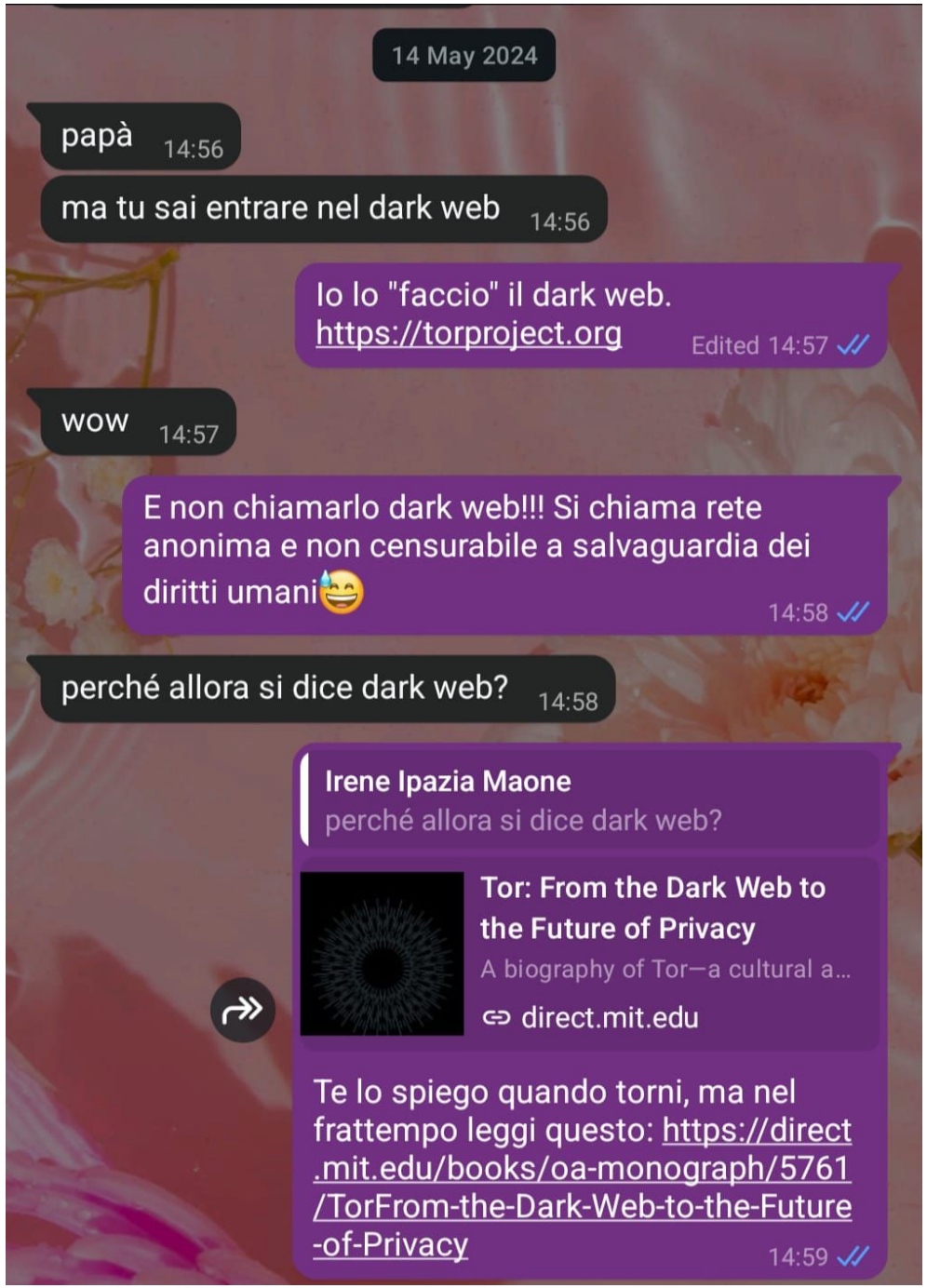
The Tor Project
Digital Rights are Human Rights

torproject.org



Tor spiegato ai miei figli

perché la privacy online non è (ancora) una causa persa


14 May 2024
papà 14:56
ma tu sai entrare nel dark web 14:56
Io lo "faccio" il dark web.
https://torproject.org
Edited 14:57
wow 14:57
E non chiamarlo dark web!!! Si chiama rete anonima e non censurabile a salvaguardia dei diritti umani
14:58
perché allora si dice dark web? 14:58
Irene Ipazia Maone
perché allora si dice dark web?
Tor: From the Dark Web to the Future of Privacy
A biography of Tor—a cultural a...
direct.mit.edu
Te lo spiego quando torni, ma nel frattempo leggi questo: https://direct.mit.edu/books/oa-monograph/5761/TorFrom-the-Dark-Web-to-the-Future-of-Privacy
14:59

Giorgio Maone

ma1

(he/him)

- creator of NoScript
- security breaker & builder
- digital rights advocate & secular humanist activist
- casting spells on Tor Browser at TPI
- elected member of the Tor Community Council



DARK WEB???

La privacy nella vita di ogni giorno

Lo spazio domestico

In casa chiudiamo le tende e la porta a chiave. Non perché nascondiamo attività illecite, ma per proteggere l'intimità affettiva e la serenità della nostra famiglia.

La casa digitale

Online lasciamo le "finestre spalancate": ricerche sanitarie, abitudini , preferenze (anche sessuali), acquisti e spostamenti vengono continuamente registrati ed elaborati.

Una battaglia in salita

Tutelare la vita digitale della famiglia significa prevenire la profilazione commerciale aggressiva e difendere il diritto di crescere senza sorveglianza.

INFRASTRUTTURA WEB

Come veniamo tracciati ad ogni click

Il modello di business dell'attenzione

Quando visitiamo un sito web standard, decine di soggetti terzi raccolgono i metadati della nostra connessione senza un reale consenso.

Metadati esposti ad ogni richiesta:

Indirizzo IP geografico • Configurazione dispositivo • Risoluzione schermo • Font installati • Orari di attività quotidiana

Fornitori di Connessione (ISP)

Memorizzano l'elenco completo dei domini e dei siti visitati ogni giorno.

Broker di Dati e AdTech

Incrociano la cronologia per costruire profili psicografici dettagliati.

Piattaforme Centralizzate

Centralizzano le identità digitali vincolando servizi essenziali al tracciamento.

DEBUNKING • FALSO MITO 1

“Se non fai nulla di male, non hai nulla da nascondere”

L'equivoco della riservatezza

Confondere la privacy con il segreto illecito è un errore logico. Avere la porta del bagno chiusa a chiave non significa compiere azioni illegali.

Libertà di pensiero

Senza privacy non esiste libertà di opinione. Sapere di essere osservati altera il comportamento spontaneo, inducendo all'autocensura.

Tutela dei soggetti deboli

Anche chi non ha nulla da nascondere beneficia di un ambiente riservato che protegge gli altri: minori, pazienti, giornalisti e ricercatori.

PRINCIPI FONDAMENTALI

Cos’è la vera ~~sovranità~~ indipendenza digitale?

Fuga da big tech

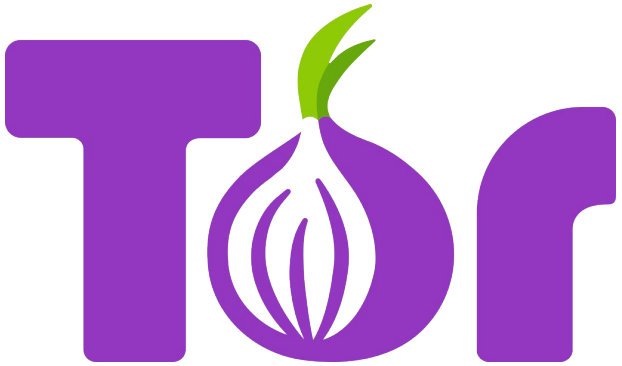
Delegare la gestione dei propri dati a poche multinazionali significa accettare regole unilaterali, tracciamento continuo e perdita di controllo sui propri contenuti.

Autodeterminazione

Decidere autonomamente quali dati condividere, con chi e per quale scopo, riappropriandosi delle tecnologie e scegliendo standard aperti e verificabili.

Software Libero e comunità

Il codice sorgente ispezionabile garantisce che non vi siano backdoor o funzionalità nascoste a danno degli utenti.



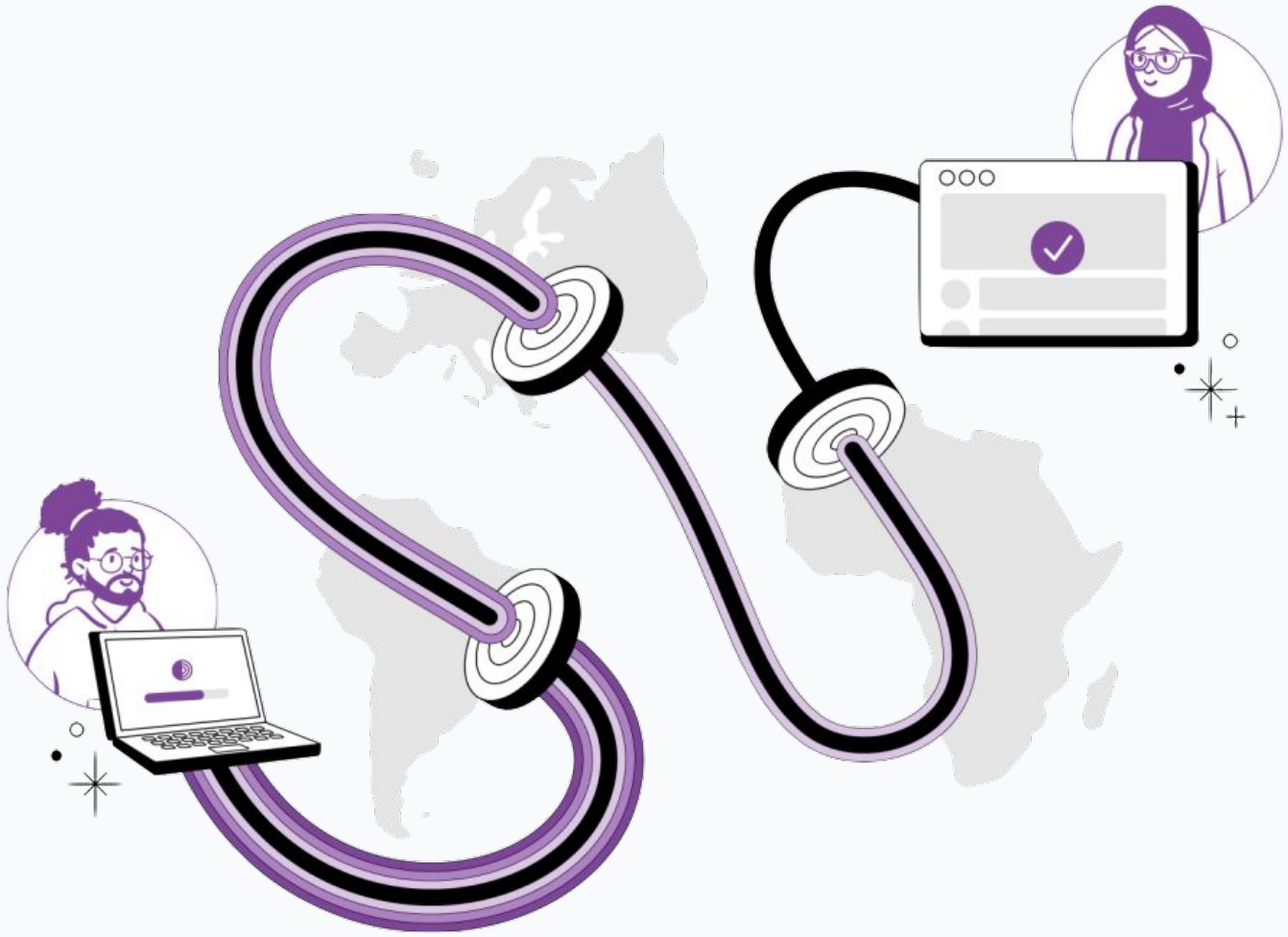
IL ~~PERSONALE~~ DIGITALE

È

POLITICO

ARCHITETTURA

Il funzionamento delle tre “sfoglie di cipolla”



Guard Relay (Ingresso)

Vede il tuo vero indirizzo IP, ma rimuove il primo strato di cifratura e non conosce la destinazione finale.

Middle Relay (Intermedio)

Rimuove il secondo strato. Isola completamente l'ingresso dall'uscita per evitare la correlazione dei dati.

Exit Relay (Uscita)

Toglie l'ultimo strato e invia la richiesta al sito. Il sito vede l'IP del nodo di uscita, mai il tuo.

DEBUNKING • FALSO MITO 2

“Tor serve solo per attività illegali”

La realtà dei dati d'uso

Oltre il **95% del traffico globale di Tor** è diretto verso il web normale (.com, .org, siti di notizie, banche), utilizzato da persone che desiderano semplicemente evitare il tracciamento.

Tor è un'infrastruttura di protezione neutrale, come la cifratura HTTPS o le reti stradali.

Associazioni e servizi critici

Organizzazioni come la Croce Rossa e Amnesty offrono portali Tor ufficiali.

Testate Giornalistiche

New York Times e The Guardian usano Tor per proteggere le loro fonti.

STORIA

Le 3 vite dell'Onion Routing

1995

Ricerca della Marina USA

Paul Syverson, Michael Reed e David Goldschlag inventano la cifratura a cipolla al Naval Research Lab per proteggere i dati d'intelligence.

2002

Sviluppo Alpha & EFF

Roger Dingledine e Nick Mathewson rilasciano il codice open source. La Electronic Frontier Foundation garantisce i primi finanziamenti.

2006

The Tor Project Inc.

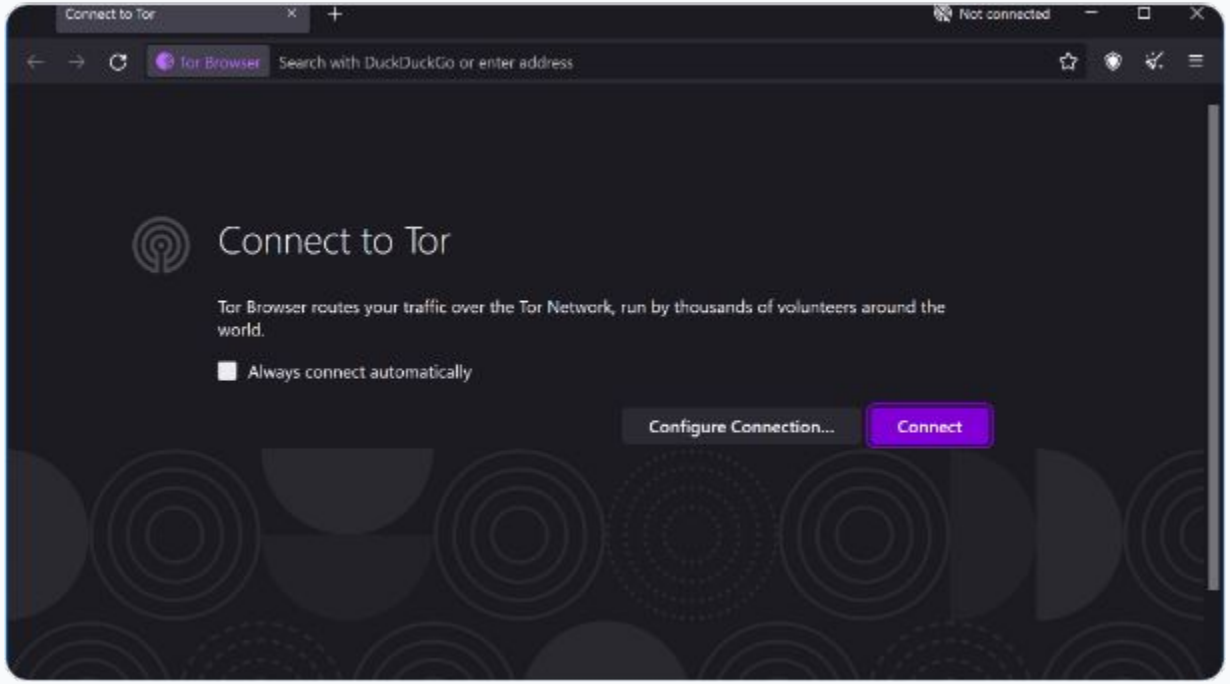
Nasce la società no-profit 501(c)(3) dedicata allo sviluppo, al mantenimento e alla difesa dei diritti umani digitali nel mondo.



Tor

STRUMENTI PRATICI

Tor Browser:
navigazione riservata, esplorazione libera

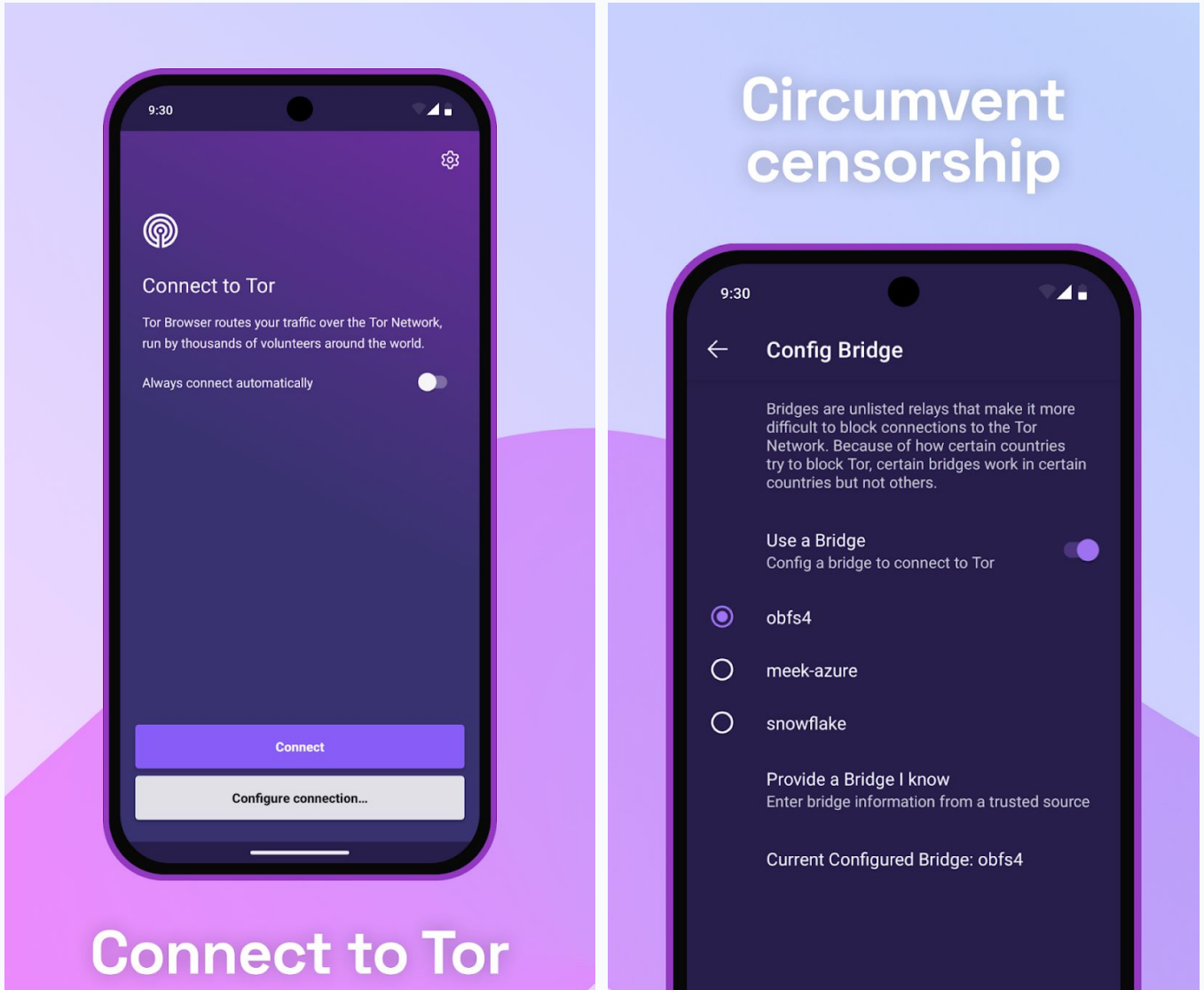


Fork di Firefox con oltre 400 patch per:

- Obbedienza al proxy
- Isolamento dei Circuiti
  Rimozione telemetria
  Prevenzione tracciamento
- Fingerprinting-resistance

STRUMENTI PRATICI

Tor Browser:
navigazione riservata, esplorazione libera



Fork di Firefox con oltre 400 patch per:

- Obbedienza al proxy
- Isolamento dei Circuiti
  Rimozione telemetria
  Prevenzione tracciamento
- Fingerprinting-resistance

PREVENZIONE

Blocco preventivo dell’esecuzione di codice non autorizzato





NoScript nel Tor Browser

JavaScript può essere utilizzato per estrarre dati dal browser, identificare i componenti hardware o sfruttare vulnerabilità per rivelare il reale IP dell'utente.

Livello Standard

Tutte le funzionalità web sono attive per la massima compatibilità.

Livello Più Sicuro (Safer)

Disattiva JavaScript sui siti HTTP non cifrati e disabilita alcuni font ed elementi multimediali.

Livello Il Più Sicuro (Safest)

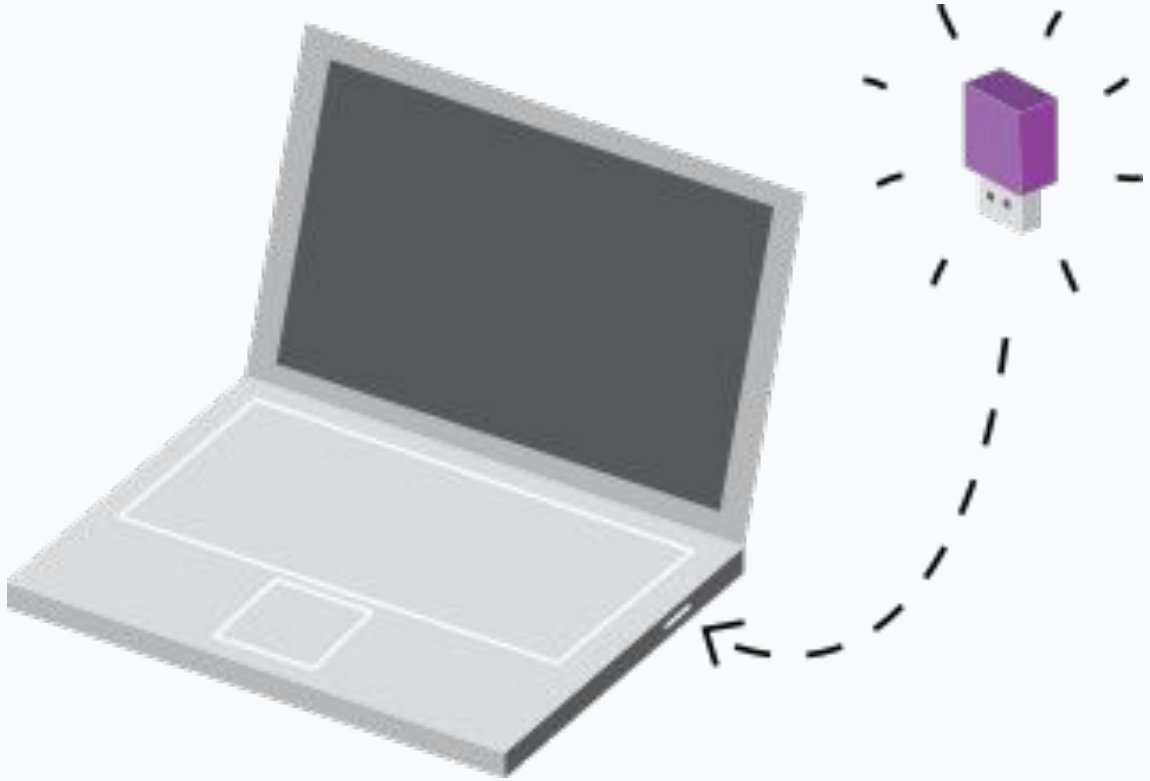
Blocca di default tutti gli script JS su qualunque sito, consentendo solo testo e immagini statiche.

SISTEMI OPERATIVI

Tails OS: riservatezza totale su chiavetta USB

The Amnesic Incognito Live System

Tails è una distribuzione Linux basata su Debian, portatile che si avvia da supporto esterno senza modificare il sistema operativo ospitante.



Cancellazione automatica della RAM

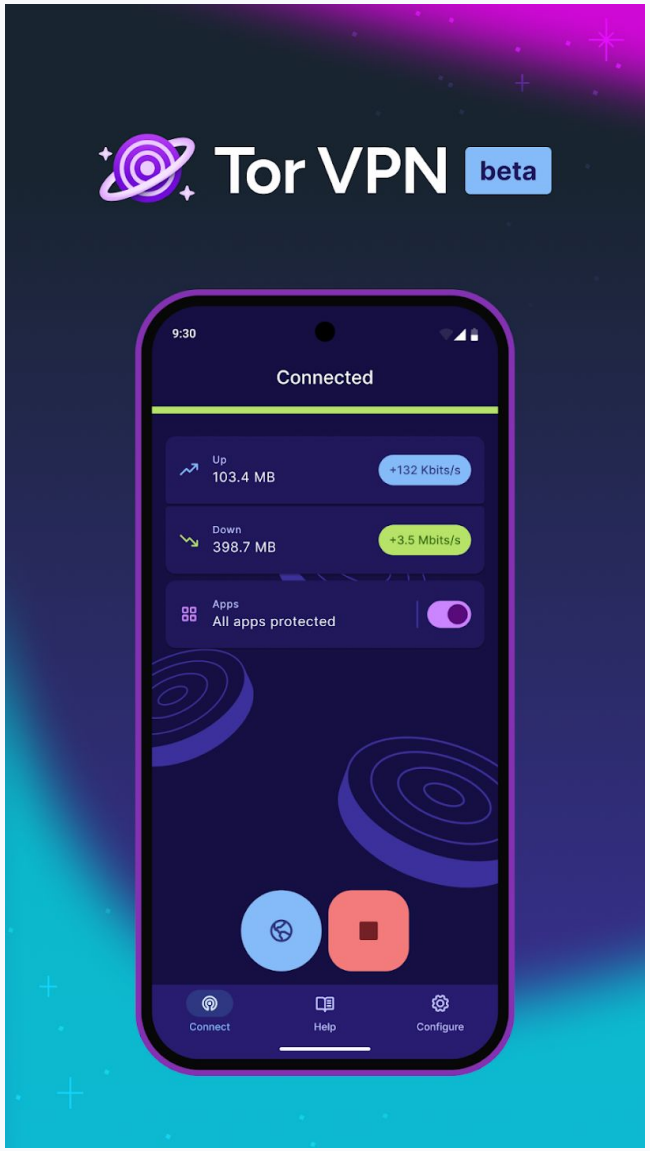
Al momento dello spegnimento, ogni modifica scompare, eliminando le tracce d'uso sul computer.

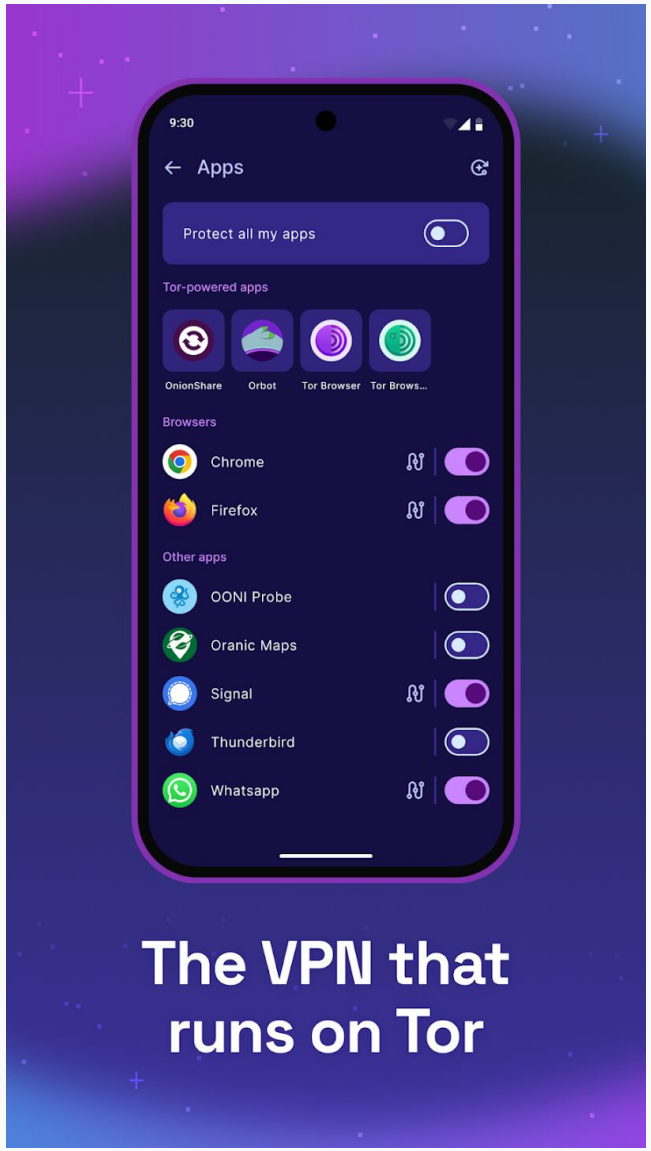
Tor di sistema

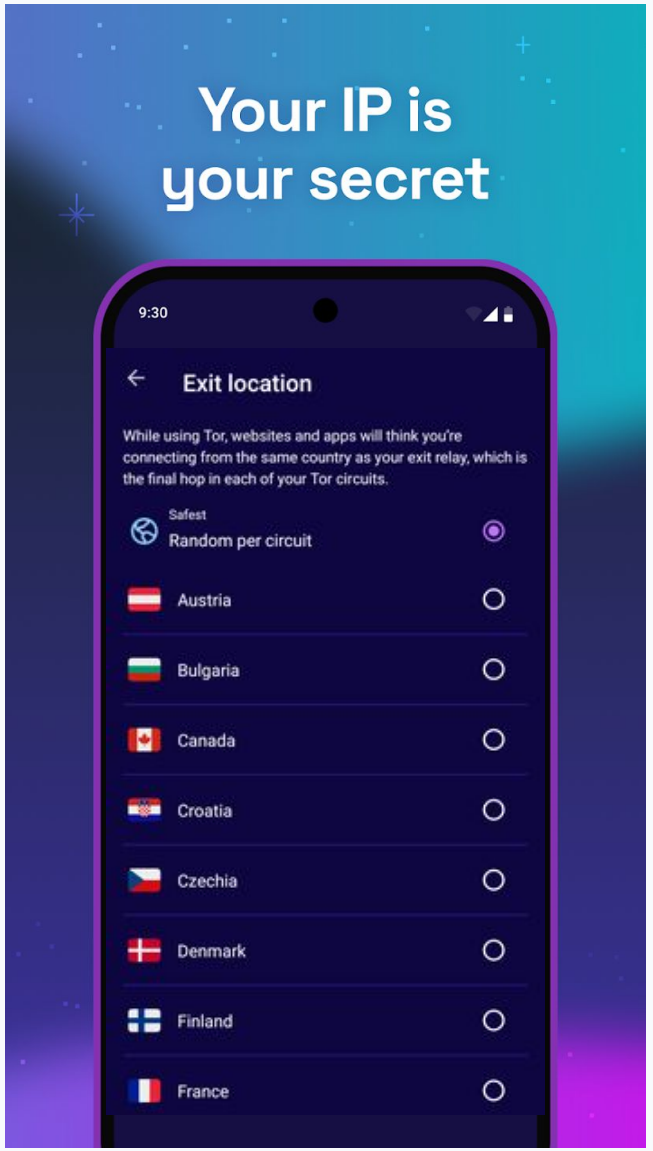
Tutta l'attività di rete passa attraverso Tor

APPLICAZIONI MOBILI

TorVPN: entra nel tunnel con tutto il tuo smartphone







RESISTENZA ALLA CENSURA

I servizi trasparenti .onion

Indirizzi crittografici

Gli indirizzi .onion sono generati direttamente dalle chiavi pubbliche del server, garantendo l'autenticità del sito senza autorità di certificazione esterne.

Connessione End-to-End

Il traffico non esce mai dalla rete Tor: la connessione rimane cifrata dall'utente fino al server di destinazione senza l'uso di nodi d'uscita.

Protezione del servizio

Nasconde la collocazione dei server di pubblicazioni indipendenti da censura o sequestri arbitrari.

RESISTENZA ALLA CENSURA

Bridges e Snowflake: Superare i blocchi di rete

Bridges (nodi ponte)

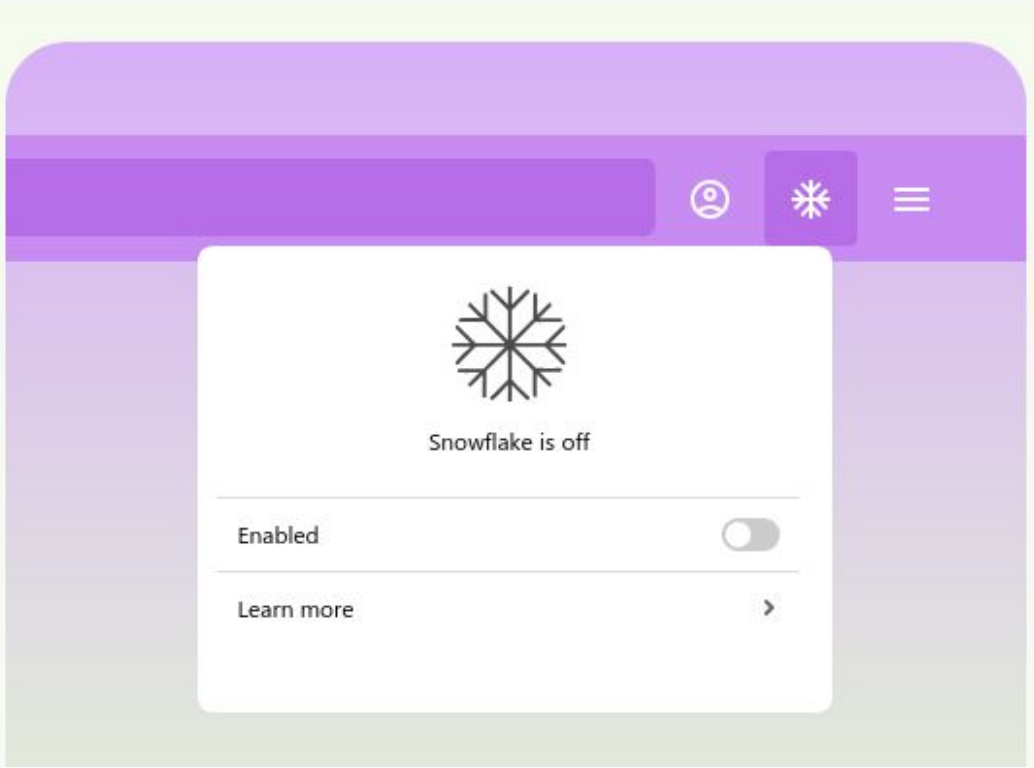
Pluggable Transports (obfs4, meek)

Relay non elencati nei elenchi pubblici ufficiali di Tor, fondamentali quando l'accesso ai nodi noti viene bloccato dai firewall di stato.

Snowflake

Supporto immediato da qualsiasi utente web

Sfrutta le connessioni WebRTC dai browser di volontari per mascherare il traffico Tor come una normale chiamata audio/video.



APPLICAZIONI REALI

I contesti d’uso fondamentali nel mondo

Whistleblowing

Piattaforme come SecureDrop consentono ai dipendenti di denunciare corruzione ed illeciti aziendali in totale sicurezza.

Supporto Psicologico

Consente a vittime di violenza domestica o minoranze di cercare aiuto e informazioni sanitarie senza lasciare tracce in casa.

Aree di Crisi

Permette ai cittaadini di comunicare con familiari all'estero durante blackout informativi o conflitti armati.

INFRASTRUTTURA PARTECIPATA

Una rete sostenuta da volontari in tutto il mondo

Senza server centrali di proprietà

La rete Tor si basa sulla generosità di individui, università, associazioni e aziende che mettono a disposizione oltre **9.000 nodi attivi** nel mondo.

Decentralizzazione come difesa

Nessuna singola entità può controllare o spegnere la rete, poiché la gestione è distribuita su diverse giurisdizioni internazionali.

9.000+

Relay attivi distribuiti nel mondo

2.500+

Bridges anti-censura attivi

IGIENE DIGITALE

Consigli pratici per la tutta la famiglia

1. Separazione dei contesti

Usa browser differenti per le attività quotidiane personali e per le ricerche sensibili. Ancora meglio, **usa il Tor Browser!**

2. Gestori di password open source

Evita il riutilizzo delle credenziali.

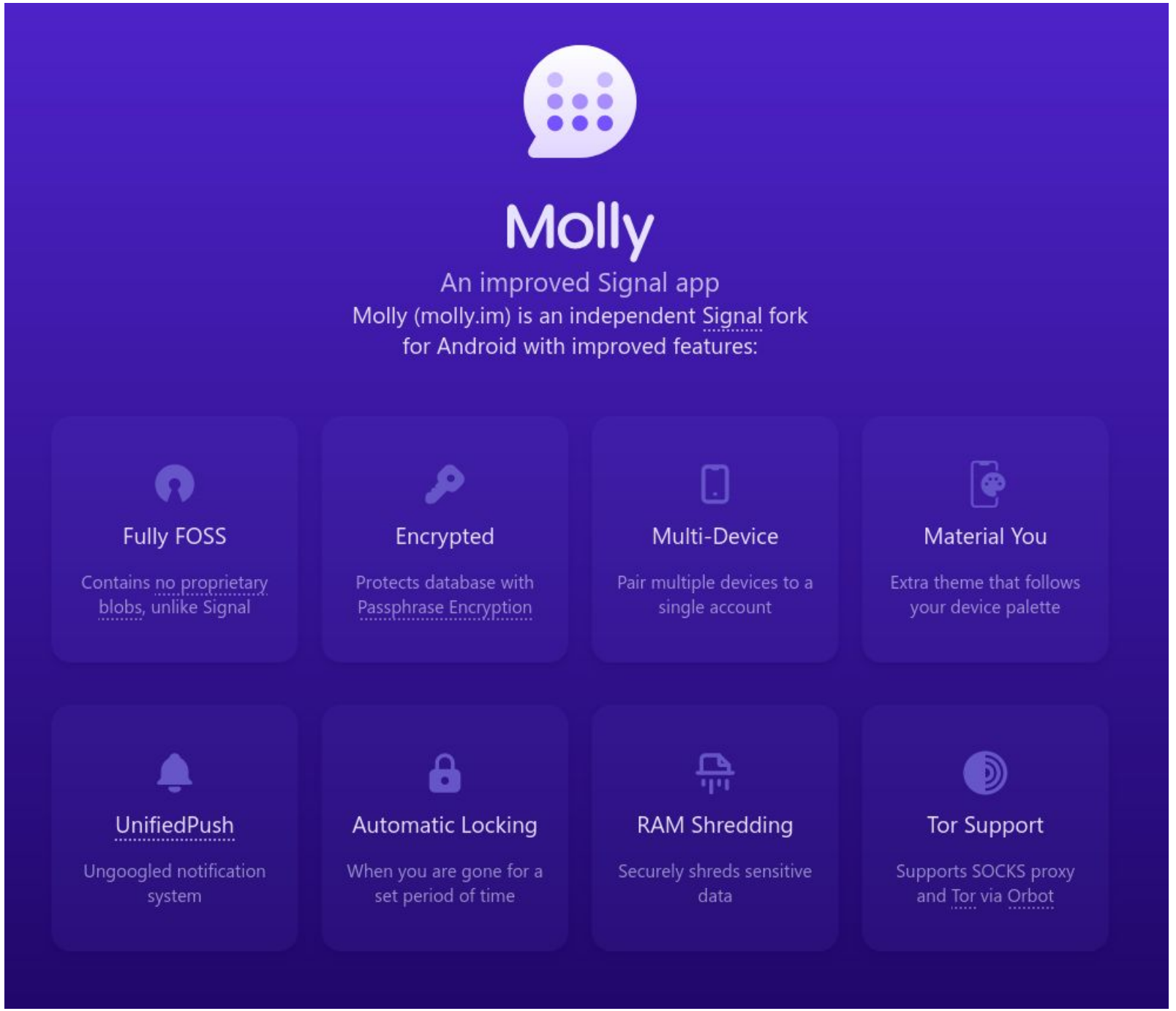
3. Motori di ricerca rispettosi

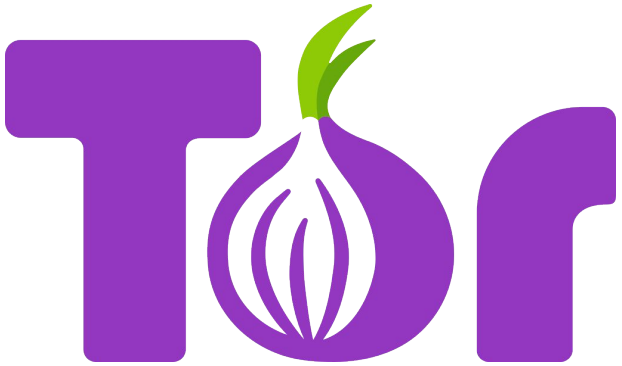
Sostituisci i motori di ricerca commerciali con alternative come DuckDuckGo



Educare alla consapevolezza

Insegnare ai propri figli l'importanza della riservatezza non significa promuovere la segretezza verso i genitori, ma fornire loro le competenze utili a difendersi dalle insidie del tracciamento , commerciale **e non**.


Molly
An improved Signal app
Molly (molly.im) is an independent Signal fork for Android with improved features:
Fully FOSS
Contains no proprietary blobs, unlike Signal
Encrypted
Protects database with Passphrase Encryption
Multi-Device
Pair multiple devices to a single account
Material You
Extra theme that follows your device palette
UnifiedPush
Ungoogled notification system
Automatic Locking
When you are gone for a set period of time
RAM Shredding
Securely shreds sensitive data
Tor Support
Supports SOCKS proxy and Tor via Orbot



SE TU NON TI OCCUPI DELL'**AI**...

AMBITO ACCADEMICO

Il valore della ricerca accademica per Tor

Laboratorio di Ricerca

Tor rappresenta il principale banco di prova accademico per gli studi sulla crittografia applicata, sui sistemi distribuiti e sulla resistenza alla censura.

Protezione Legale

Gli atenei offrono un quadro normativo e d'indipendenza unico, fondamentale per gestire infrastrutture di rete aperte senza ingerenze esterne.

Banda ad Alta Velocità

Le connessioni ad altissima capacità degli atenei migliorano notevolmente le prestazioni complessive della rete globale.

ADESIONE UNIVERSITARIA • PARTE 1 DI 3

EFF Tor University Challenge

L'iniziativa della Electronic Frontier Foundation

La campagna sfida le università e i gruppi studenteschi a configurare ed ospitare nodi di transito o d'uscita per rafforzare la privacy globale.

L'obiettivo della sfida

Aumentare la capacità della rete, migliorare i tempi di risposta e riaffermare il ruolo delle università quali difensori della libertà d'espressione.

Atenei Partecipanti

- Massachusetts Institute of Technology
- Stanford University
- Università di Cambridge
- Technische Universität München
- Decine di dipartimenti informatici nel mondo

ADESIONE UNIVERSITARIA • PARTE 2 DI 3

Modalità operative per gruppi studenteschi

OPZIONE BASE

Middle Relay

Facile da configurare, gestisce unicamente traffico interno già cifrato. Nessun rischio legale o di abuso.

CENSURE RIGIDE

Snowflake Proxy

Può essere eseguito anche dai browser delle sale macchine o dai dispositivi individuali degli studenti.

IMPATTO MASSIMO

Exit Relay

Invia traffico al web in chiaro. Si raccomanda di utilizzare le linee guida legali predisposte da EFF.

ADESIONE UNIVERSITARIA • PARTE 3 DI 3

Aderire alla challenge: Link e kit legali

1. **Scarica la documentazione di EFF**
   Comprende template di richiesta ed indicazioni legali per il responsabile di rete dell'ateneo.

2. **Coinvolgi i docenti di dipartimento**
   Proponi l'attivazione del nodo nell'ambito dei corsi di Sicurezza Informatica o Reti.

3. **Registra il nodo nel portale EFF**
   Aggiungi il tuo ateneo all'elenco delle università partecipanti alla sfida globale.

EFF Tor University Challenge

Accedi direttamente alle risorse legali e tecniche ufficiali:

https://toruniversity.eff.org/

La riservatezza è un diritto umano fondamentale.

Inizia oggi stesso: installa Tor Browser e promuovi l'adesione al progetto nel tuo ateneo.

Partecipa alla Challenge: toruniversity.eff.org

donate.torproject.org

ma1@torproject.org

Tor: powered by you

Unlike Big Tech, Tor doesn't sell your data to make money. Instead, 6,490 donors every year keep Tor strong. Join the movement with a donation today!

Donate now ♥

