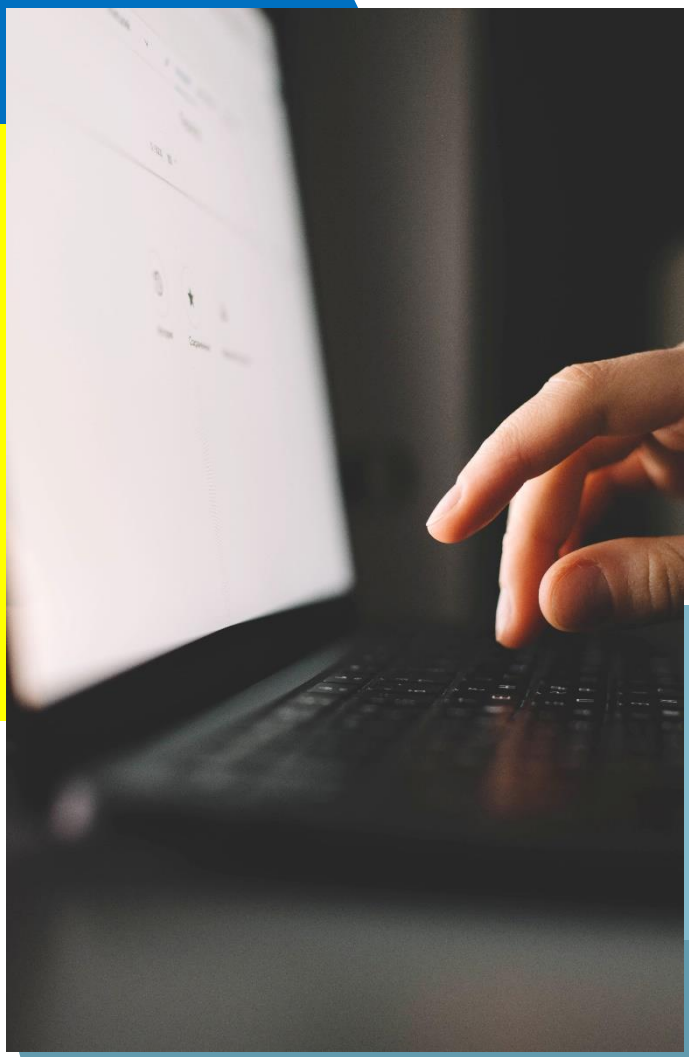
Посібник з анонімного спілкування.



Анонімність може мати вирішальне значення.

Якщо ваш власний світ перекинувся вгору дном, і вам доводиться турбуватися про те, що хтось може читати ваші листування, то через спілкування ви можете наразити на небезпеку інших людей, друзів і сім'ю. Тому важливо знати основи анонімного спілкування у зонах криз та військових дійспілкування.

Опубліковано 2022

Анонімне спілкування означає безпеку.

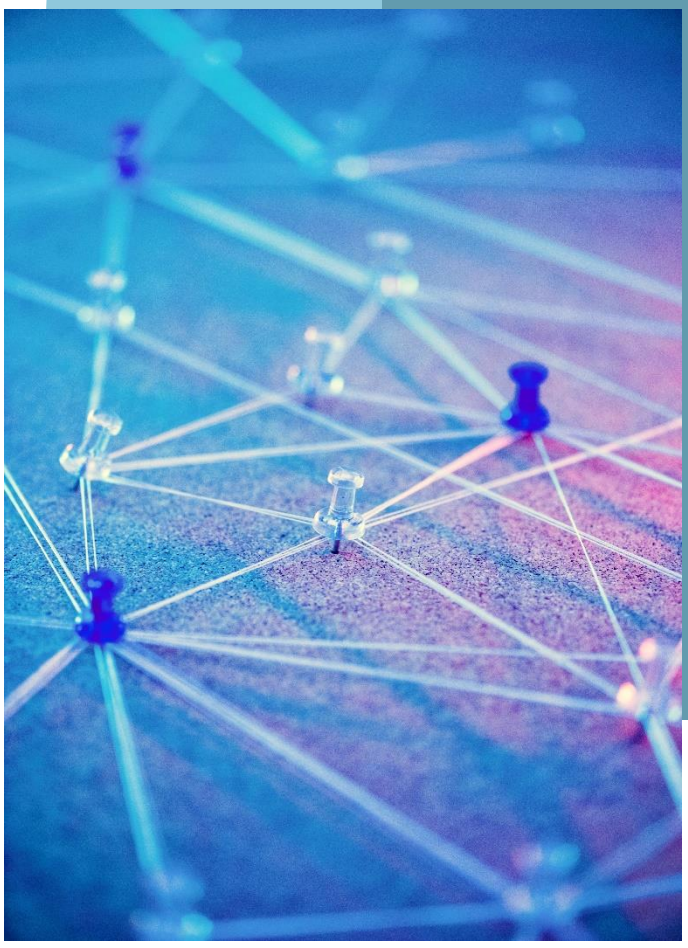


Nikolaus Stapels

За допомогою цього посібника я хотів би зробити свій внесок у підтримку людей у кризових зонах і зонах бойових дій. Під час кризи я зміг допомогти багатьом біженцям налагодити анонімне спілкування в зонах бойових дій

Програмне забезпечення VPN під державною цензурою

Деякі країни обмежують доступ до безкоштовної інформації в Інтернеті. Програмне забезпечення VPN є хорошим першим кроком, оскільки ви можете налаштувати зашифровану лінію за допомогою програмного забезпечення VPN і таким чином, наприклад, обійти так звані блоки DNS і отримати доступ до заблокованих веб-сайтів.



Підключення VPN також захищає вашу конфіденційність в Інтернеті, змінюючи власну IP-адресу, що ускладнює ідентифікацію.

Крім того, ваше спілкування неможливо або важко перехопити і, наприклад, змінити.

Ви можете використовувати звичайні пошукові системи для смартфонів, планшетів або ноутбуків, щоб бути ще безпечнішими та анонімнішими в Інтернеті.

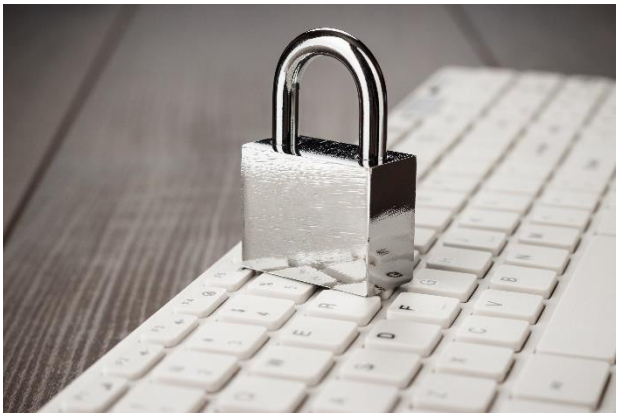
Мережа TOR

У світі, який оцифровується все швидше й швидше, також швидко зростають можливості для моніторингу окремих осіб, груп людей або цілих груп населення.

Це вже не лише журналісти, які проводять вибухові дослідження, і правозахисники, які хочуть залишатися анонімними, спілкуючись один з одним. «Звичайним» користувачам також все частіше доводиться вживати заходів безпеки, щоб захистити себе та своїх близьких.
Чудовим і простим варіантом є використання мережі TOR, оскільки пакети даних не надсилаються безпосередньо до веб-сервісу, а обходять через різні сервери в мережі.

Мережа TOR

За допомогою браузера TOR ви можете повністю автоматично встановити анонімне з'єднання з мережею і таким чином затерти свої сліди.
Ця техніка анонімізації називається «лукова маршрутизація»; веб-сайти маршрутизуються через так звані «вузли».
Це з'єднання зашифровано, тому захищає вашу особу.
Крім того, таким чином можна



Захистіть всі свої комунікації

Використання мережі TOR; Давайте розпочнемо.

Коли Інтернет більше не пропонує безпечних каналів, багато користувачів переходять на мережу TOR. TOR добре відомий завдяки широкому спектру користувачів, а програмне забезпечення легко знайти за допомогою популярних пошукових систем.

При необхідності переконайтеся, що ви завантажуєте програмне забезпечення через загальнодоступну точку доступу, наприклад, завантажте у свій мобільний телефон, ноутбук або планшет, а потім роздайте через USB-накопичувач, якщо це необхідно, щоб ніякі органи спостереження не помітили, що ви безпосередньо завантажили браузер TOR .
Чим більше людей навколо вас використовують мережу TOR, тим безпечнішим для всіх

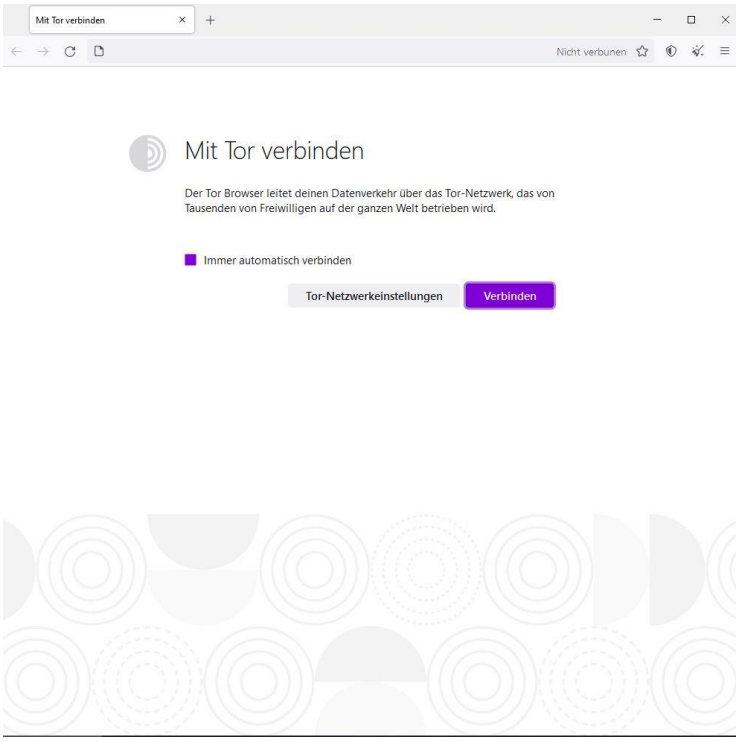
Початок

Після встановлення та запуску браузера ви можете підключитися безпосередньо до мережі TOR.

Заходити в налаштування мережі TOR (ліва кнопка) потрібно лише в тому випадку, якщо браузер TOR заблоковано через обмеження у вашій країні.

У цьому випадку необхідно встановити так звані мости;

Додаткову інформацію можна знайти безпосередньо за адресою: https://bridges.torproject.org/



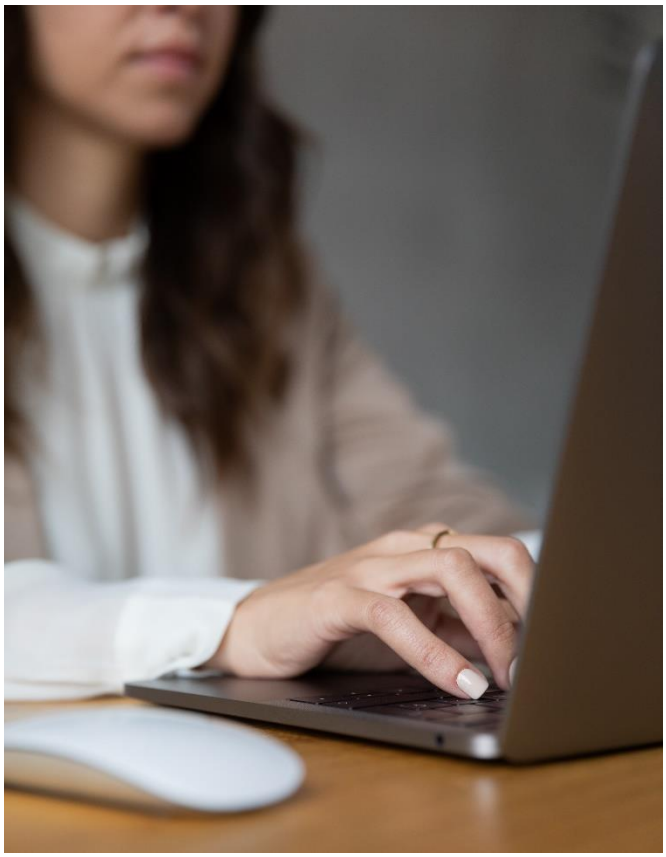
Головний екран TOR Browser

Важливі зауваження щодо використання

З технічної точки зору, анонімність дуже легко реалізувати, оскільки більшість речей працює повністю автоматично.

Але є одна велика небезпека – деякі помилки, які багато користувачів роблять на початку.
Тому зверніть увагу на наступні моменти:

- Створення нових (анонімних) акаунтів у соціальних мережах; вас можна впізнати за старим.
- Не використовуйте справжні імена чи існуючі псевдоніми (нікнейми) з інших сайтів.
- Не вводьте справжні або існуючі адреси електронної пошти.
- Не використовуйте файли cookie під час серфінгу в мережі TOR, ви можете відмовитися від них прямо в браузері.
- Продовжуйте захищати свої комп'ютери за допомогою антивірусного програмного забезпечення і брандмауерів.



IT-Безпека

Хоча ви можете переглядати сторінки анонімно та вільно переміщатися по мережі TOR, зверніть увагу, що ваші дані, як і раніше, зберігаються у незашифрованому вигляді на вашому пристрої і тому можуть бути прочитані третіми особами.

Навігація

Навігація в мережі TOR не така комфортна, як у звичайному Інтернеті.

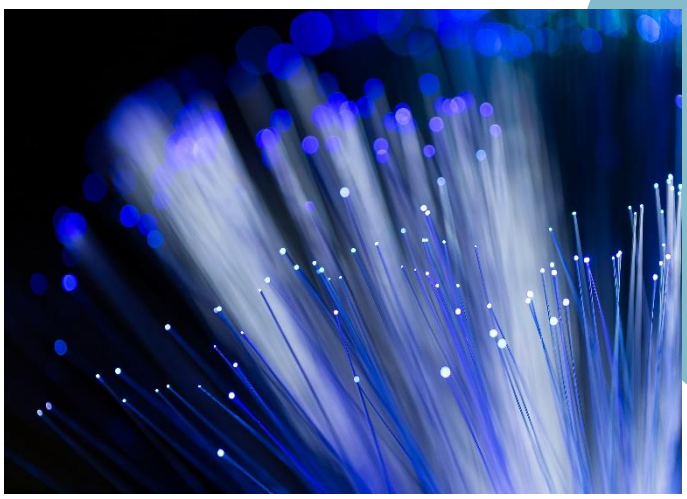
Однак за допомогою браузера TOR ви також можете відкрити звичайні веб-сайти, а отже, також пошукові системи та шукати там конкретні послуги.

У результаті ви повинні переконатися, що отримуєте веб-сайти з розширенням .onion.

Так само, як різні веб-сайти можуть містити такі розширення, як .de або .com, усі веб-сайти в мережі TOR мають розширення .onion.

Потім ви зможете отримати доступ до цих сторінок за допомогою браузера TOR і анонімно переглядати їх.

Закінчення .onion повідомляє, що веб-адреса знаходиться в мережі TOR



Деякі веб-сайти TOR

Пошта

ProtonMail

Користувачі можуть надсилати та отримувати електронні листи анонімно через провайдера..

Також є вільний доступ.

Посилання на мережу TOR

Пошукова система

DuckDuckGo

Це пошукова система, яка забезпечує високий рівень конфіденційності.

Зауважте, що пошук у темній мережі часто не працює, оскільки сайти офлайн

Link ins TOR-Netzwerk

Посилання на мережу TOR

Link= посилання

Соціальни мережі

Facebook

Багато користувачів перебувають у Соціальних мережах, таких як Facebook.

Тому Facebook також переніс свій сервіс у мережу TOR. При необхідності шукайте додаткові послуги.

.

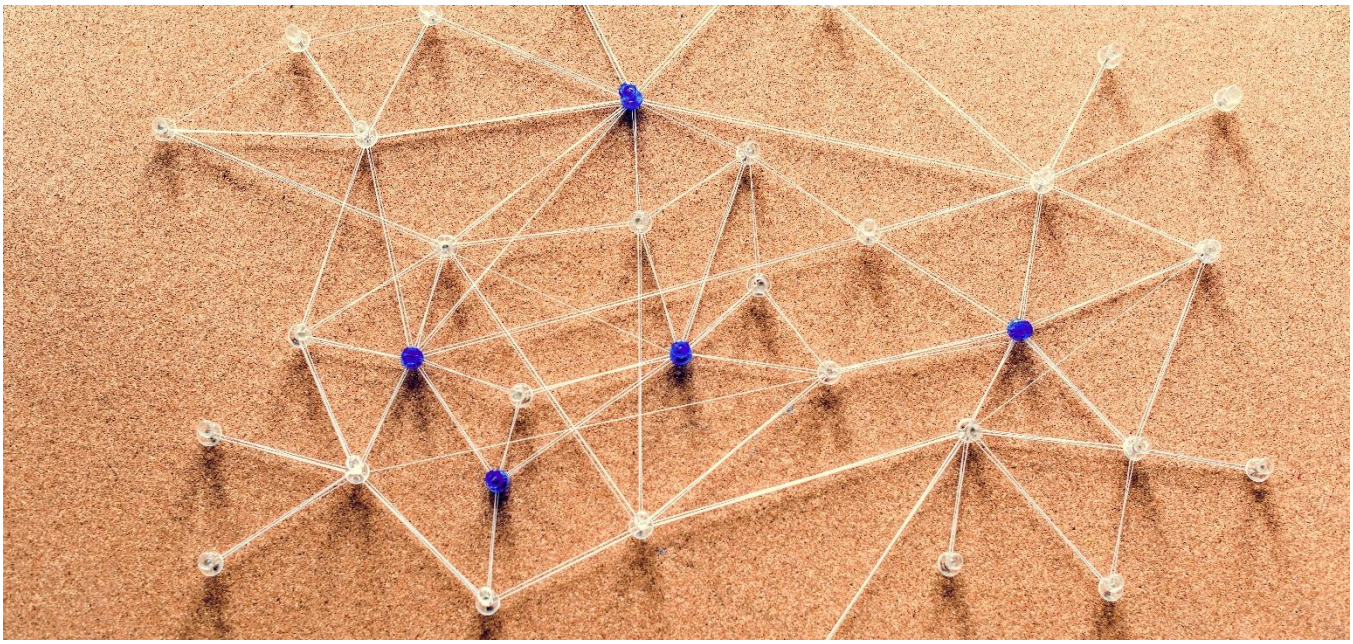
Посилання на мережу TOR

Новини

SecureDrop

Документами та файлами можна поділитися з медіа-організаціями по всьому світу через SecureDrop

Посилання на мережу TOR



Які існують «безпечні» послуги месенджера ?



По суті, ви завжди повинні покладатися на безпечний месенджер, незалежно від повідомлень. Але особливо в умовах кризи чи війни ви повинні звертати більше уваги на дані, які ви надсилаєте, і програмне забезпечення, яке використовуєте. Ось кілька месенджерів як приклад:

Signal

Сам Едвард Сноуден рекомендував використовувати Signal, оскільки цей сервіс месенджерів вважається одним із найбезпечніших у світі.
Шифрування було перевірено кілька разів і працює добре.

Threema

Threema походить зі Швейцарії, і саме там розташовані сервери. Серед іншого, провайдер обіцяє високий рівень безпеки та захисту даних через розташування серверів.



Telegram

Цей месенджер також покладається на наскрізне шифрування (активуйте його), щоб треті сторони не могли його прочитати. Однак проект не повністю відкритий (не на 100% перевірений третіми сторонами).

У вас є які-небудь питання?



Ми раді підтримати вас
info@cyber-fuchs.de
Наша пошта у розпорядженні для ваших запитів

Цей посібник призначений для того, щоб зорієнтувати вас і допомогти безпечно спілкуватися.
Ми не заглиблювались у технічні подробиці щоб дати вам зрозумілий первинний огляд.