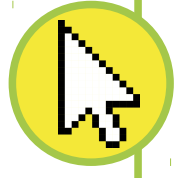
TorProject.org

La Misión de Tor

El Proyecto Tor crea y distribuye herramientas libres que permiten a periodistas, activistas de Derechos Humanos, diplomáticos, hombres de negocios o a cualquier otra persona utilizar Internet sin ser vigilados 'online' por gobiernos o empresas.

El Proyecto Tor es también un recurso global para la tecnología, la investigación y la educación en la búsqueda de la libertad de expresión, el derecho a la privacidad 'online' y la elusión de la censura. The Tor Project está orgulloso de ser una Fundación líder en su campo.

Averigua más en
https://www.torproject.org/



Únete a nosotros

Necesitamos tu ayuda para continuar el esfuerzo global por la libertad de expresión, el derecho a la privacidad 'online' y la elusión de la censura. Únete a nosotros como patrocinador voluntario, aportador o para eventos futuros dirigidos por el equipo de Tor.

Lo que Tor hace mejor

- Proporciona privacidad 'online'
- Derrotar la censura
- Protejer periodistas
- Protejer defensores de los Derechos Humanos
- Protejer víctimas de violencia doméstica
- Mantener los canales de información 'online' globales abiertos para todos
- Trabajar con legisladores
- Asociarse con instituciones académicas e investigadoras

Los Cuerpos Policiales y Tor

¿Quién usa Tor?

La gran mayoría de los usuarios de Tor son ciudadanos ordinarios que quieren mantener el control de su privacidad 'online', o usuarios censurados que necesitan eludir el bloqueo de Internet. Los criminales que quieren romper la ley ya tienen opciones más efectivas que Tor.

Sin registro ni puertas traseras

Los usuarios de Tor pueden fiarse de la privacidad del mismo. Por diseño, el operador de un repetidor o alguien con acceso físico al mismo no puede conocer la dirección IP de un usuario de Tor. La revisión continua del código fuente de Tor por las comunidades académica y 'open source' garantizan que no hay puertas traseras en Tor.

Líneas de aviso anónimas

Tor proporciona la infraestructura más segura para una línea de soplos 'online' realmente anónima, crítica para mantener seguros los canales de comunicación para testigos e informantes.

Operaciones encubiertas

Agencias policiales e investigadores utilizan Tor para contolar anónimamente las páginas web y servicios de los sospechosos. Al ocultar las identidades y localizaciones de los investigadores, Tor puede ser una herramienta valiosa para las operaciones encubiertas 'online'.

Cómo funciona Tor

Alicia cifra su solicitud de la página web de Blas tres veces, y la envía al primer repetidor.

El primer repetidor quita la primera capa de cifrado pero no sabe que la solicitud de página web es para Blas.

El segundo repetidor quita otra capa de cifrado y reenvía la solicitud de página web.

El tercer repetidor quita la tercera capa de cifrado y reenvía la solicitud de página web a Blas, pero no sabe que viene de Alicia.

Blas no sabe que la solicitud viene de Alicia, a menos que ella se lo diga.

Saber más

- El compromiso de Tor con la enseñanza incluye policías y legisladores.
- Los canales de documentación y ayuda de Tor están abiertos para cualquiera.
- Aprenda cómo utilizar el servicio ExoneraTor para averiguar si una dirección IP fue utilizada por un repetidor Tor.
- Aprenda más preguntando al equipo de expertos de Tor.

https://www.torproject.org/

Beneficios del anonimato 'online'

La realidad

Los proveedores de servicio de Internet (como Movistar u ONO), sitios web (como Google y Facebook), y gobiernos utilizan una forma común de vigilancia por internet conocida como seguimiento de direcciones IP para vigilar las conversaciones en redes públicas.

- Los sitios de noticias pueden propocionar artículos diferentes basándose en tu localización.
- Los sitios de ventas pueden alterar los precios basándose en tu país o institución.
- Una persona media es seguida por más de cien compañías para vender su perfil a los anunciantes.
- Tu actividad en redes sociales puede ser revelada y usada contra ti por individuos maliciosos.

La libertad

El panorama de Internet está en constante cambio, y las tendencias legales, policiales y tecnológicas amenazan el anonimato como nunca antes, socavando nuestra capacidad para hablar y leer 'online' libremente. Los países se vigilan entre ellos y a sus ciudadanos, bloquean páginas, vigilan el tráfico y coartan importantes sitios mundiales de noticias.

Cómo funciona Tor

Alicia cifra su solicitud de la página web de Blas tres veces, y la envía al primer repetidor.

El primer repetidor quita la primera capa de cifrado pero no sabe que la solicitud de página web es para Blas.

El segundo repetidor quita otra capa de cifrado y reenvía la solicitud de página web.

El tercer repetidor quita la tercera capa de cifrado y reenvía la solicitud de página web a Blas, pero no sabe que viene de Alicia.

Blas no sabe que la solicitud viene de Alicia, a menos que ella se lo diga.

Nº1 en Privacidad 'Online'

- Tor es tecnología libre y de fuente abierta, perfeccionado a lo largo de 10 años de investigación y desarrollo por el equipo de Tor de investigadores en seguridad y programadores.
- Tor es una de las tecnologías más efectivas para proteger tu privacidad 'online' y garantizar que tu seguridad 'online' personal permanece bajo tu control.

https://www.torproject.org/

Libertad y privacidad 'online'

censura

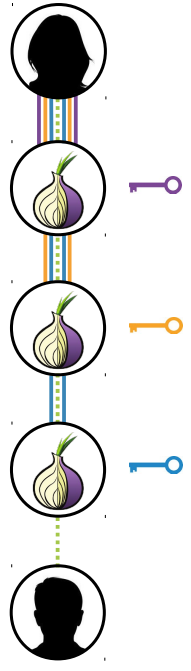
(DRAE, 23ª edición)

Intervención que practica el censor en el contenido o la forma de una obra atendiendo a razones ideológicas, morales o políticas.

Censura 'online'

En un campo de juego global, la censura toma un significado completamente nuevo. Restringir el acceso a la información y vigilar el contenido publicado es más común de lo que la gente cree. Los investigadores de la censura en Tor trabajan para crear herramientas que se mantienen por delante de las tácticas de la censura y proporcionan 'online' canales abiertos para cualquiera. El equipo de Tor crea alianzas para elevar la conciencia sobre el tema y educar a la gente en la importancia de la privacidad y la libertad de expresión 'online'.

Cómo funciona Tor



Alicia cifra su solicitud de la página web de Blas tres veces, y la envía al primer repetidor.

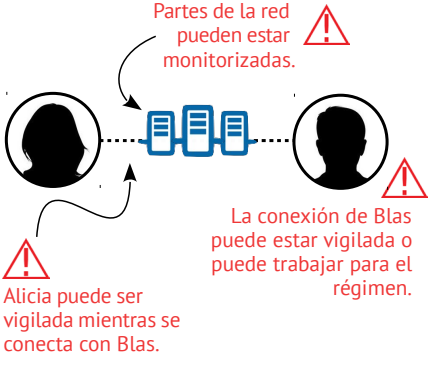
El primer repetidor quita la primera capa de cifrado pero no sabe que la solicitud de página web es para Blas.

El segundo repetidor quita otra capa de cifrado y reenvía la solicitud de página web.

El tercer repetidor quita la tercera capa de cifrado y reenvía la solicitud de página web a Blas, pero no sabe que viene de Alicia.

Blas no sabe que la solicitud viene de Alicia, a menos que ella se lo diga.

La vigilancia en Internet es común y sencilla.



Algunos diseños de elusión usan una sola capa para ocultar las conexiones.

Desafortunadamente, una capa (como con un proxy) es fácil de atacar.

https://www.torproject.org/