Blogueo Anónimo con Wordpress y Tor

Por Ethan Zuckerman

Un borrador temprano de esta guía fue escrito por Ethan Zuckerman el 13 de Abril de 2005 y actualizado el 1º de Octubre de 2006. El 8 de Agosto de 2007, Global Voices Advocacy publicó una versión actualizada, enlazable, HTML de la guía, junto con un archivo PDF descargable. El 10 de marzo de 2009, la guía ha sido actualizada de nuevo, para que todos los tips sean también compatibles con la reciente actualización de Tor.

Introducción
Una de las grandes alegrías de trabajar en Global Voices ha sido tener la oportunidad de trabajar con personas que están expresándose, a pesar de las poderosas fuerzas que trabajan para mantenerles en silencio. He trabajado con cierto número de autores que han querido escribir acerca de asuntos políticos o personales en internet, pero que sentían que no podían escribir en la red a menos que pudieran asegurarse de que a través de sus escritos no fuera posible rastrear sus identidades. Entre estos autores se incluyen activistas de derechos humanos en docenas de países, trabajadores de ayuda humanitaria en países represivos, así como denunciantes internos de compañías y gobiernos. Escribí una guía técnica sobre blogueo anónimo [ENG] algunos meses atrás y la publiqué en Global Voices, esbozando diversos métodos diferentes para bloguear anónimamente. Desde entonces, he dirigido talleres en diferentes rincones del mundo y he adquirido comodidad enseñando un conjunto particular de herramientas - Tor, Wordpress y varias cuentas de correo electrónico gratuitas-, las cuales usadas en combinación pueden proporcionar un nivel alto de anonimato. La siguiente guía no te ofrece ninguna opción -sólo te lleva a través de una solución particular, en detalle.
Puedes sentirte libre de ignorar las secciones de la guía sobre "por qué", si quieres una lectura más rápida y si eres la clase de persona que no necesita saber por qué hacer algo. Espero editar esto más bellamente en algún momento en el futuro, permitiendo que las secciones sobre "por qué" se expandan y compriman, haciendo el documento en su totalidad mucho más corto.
Si he sido poco claro en algún lugar en el documento, o si hay algo incorrecto, por favor hazme saber en los comentarios - esto es un borrador que espero pulir antes de publicarlo en Global Voices. En caso de que te sea útil y desees difundirlo más, siéntete libre -al igual que casi todo en este sitio, está bajo una licencia Creative Commons 2.5 de Atribución, lo que significa que eres libre de imprimirlo en vasos para café y venderlo, si crees que hay un mercado y puede hacerse dinero con ello.

Aclaratoria
Si sigues estas instrucciones exactamente, reducirás drásticamente las posibilidades de que tu identidad sea vinculada a tu escritura en línea a través de medios técnicos -v.g., a través de una agencia del gobierno o de la ley que obtenga registros de un proveedor de internet (ISP). Desafortunadamente, no puedo garantizarte que esto funcione en todas las circunstancias, incluyendo las tuyas, ni puedo aceptar responsabilidades penales o civiles, en caso de que el uso o el mal uso de estas instrucciones te ocasione problemas legales, civiles o personales.

Estas instrucciones no hacen nada que pueda prevenirte de ser rastreado a través de otros medios técnicos, como keylogging (la instalación de un programa en tu computadora para registrar tus pulsaciones de teclado) o vigilancia tradicional (observar la pantalla de tu computadora usando una cámara o un telescopio). La verdad es que la mayoría de la gente es vinculada con su escritura a través de mecanismos no técnicos: escriben algo que deja huellas de sus identidades, o comparten su identidad con alguien que resulta ser no confiable. No puedo ayudarte en esos frentes, excepto decirte que seas cuidadoso y listo. Para una mejor guía sobre el lado "cuidadoso y listo" de las cosas, recomiendo la guía de EFF "Cómo bloguear con seguridad [ENG]".

A lo geek:

I – Escribiendo desde computadoras compartidas

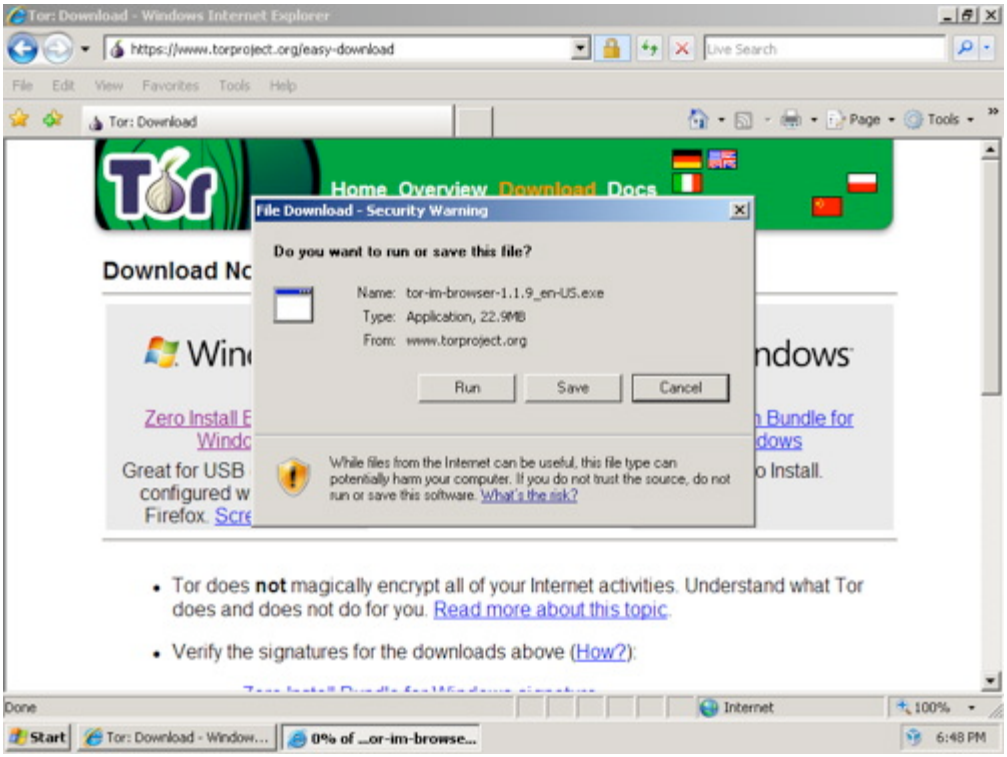
Si vas a escribir primordialmente desde computadoras compartidas (como computadoras de cybercafé) o no puedes instalar software en una computadora, por favor sigue los pasos explicados a continuación para correr el paquete del Tor Browser sin necesidad de instalar ningún software.
En caso de que vayas a bloguear principalmente desde tu computadora personal, donde puedes instalar software, por favor dirígete al capítulo II.

Paquete de Instalación desde Cero para Windows (para cualquier unidad de disco portátil)

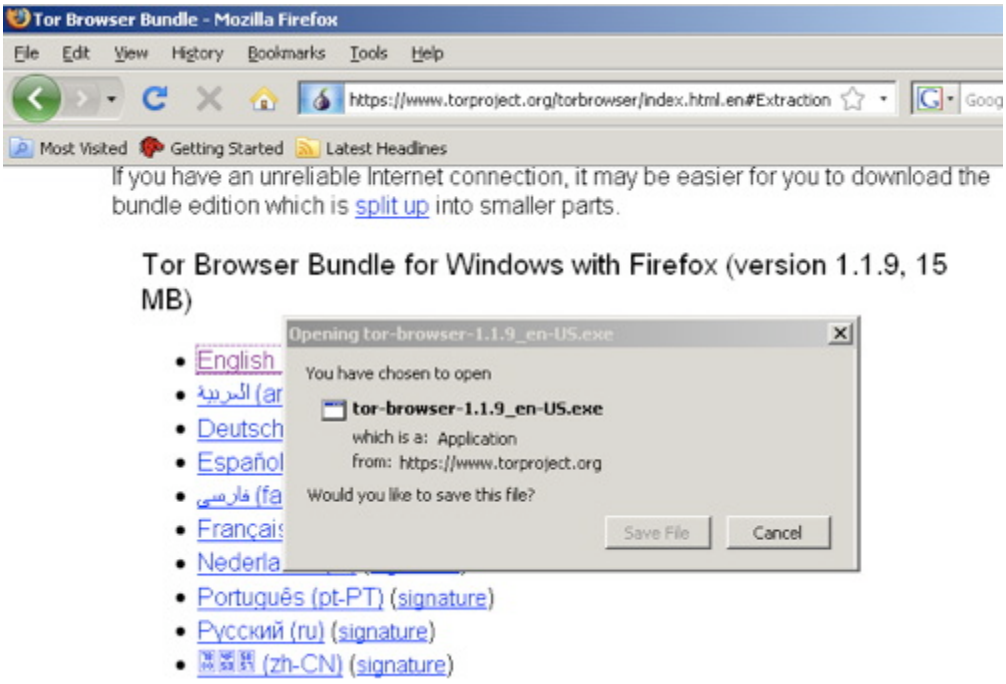
Te recomendamos que descargues el paquete de instalación desde cero (Tor Browser Bundle) para Windows, un magnífico paquete pre-configurado de Tor que contiene el navegador Mozilla Firefox para

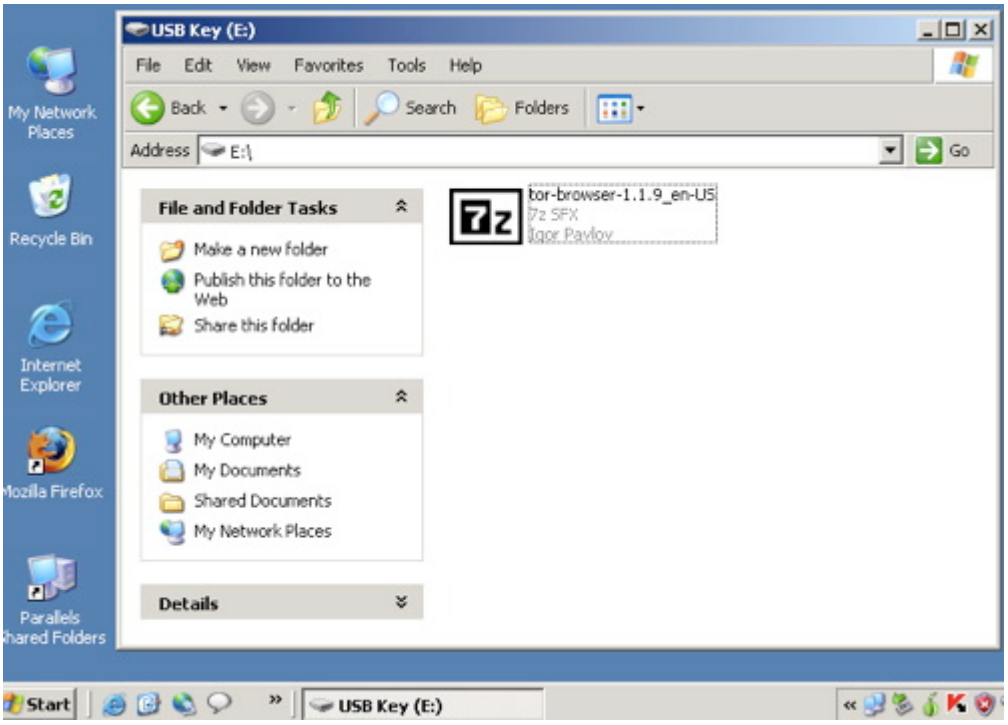
unidades USB o cualquier medio portátil (tarjeta SD, discos duros, tarjetas Flash). El Tor Browser es una versión de código abierto de un navegador portátil desarrollado por el Proyecto Tor. Es una versión altamente personalizada del navegador Firefox con Tor, Vidalia, el proxy llamado Polipo, Firefox y el Torbutton ya instalados. Está diseñado para ser instalado en una unidad USB, de modo que puedas acceder a Tor desde cualquier computadora compartida que no te permita instalar software.

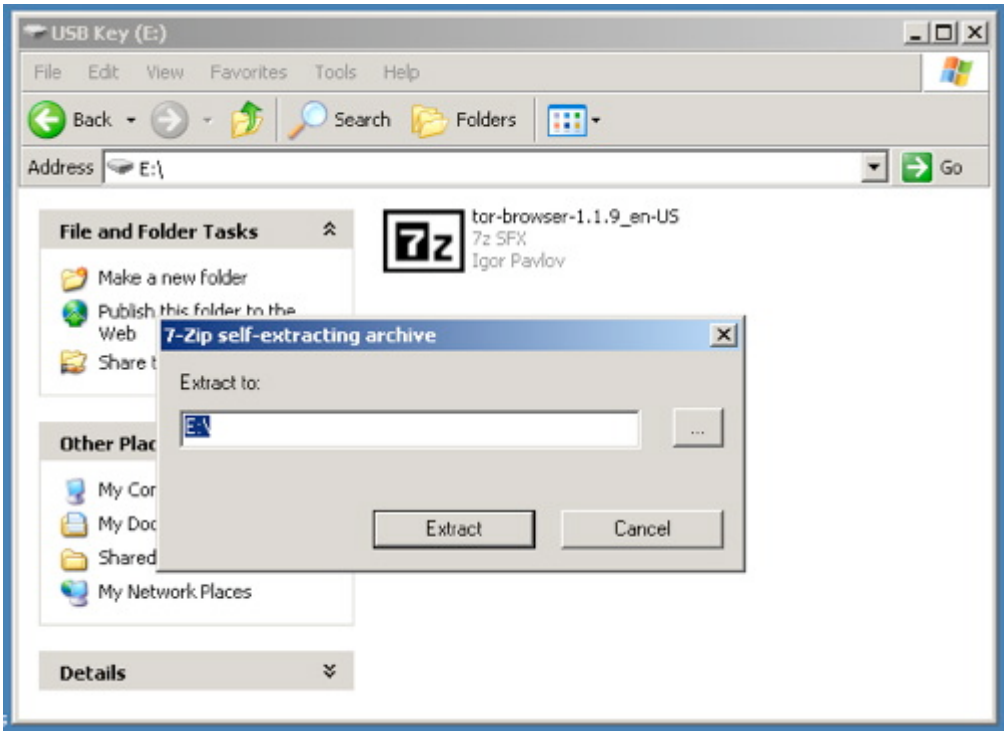
a) Descarga el Tor Browser Bundle. Descarga el paquete de tu idioma preferido desde la página web del Proyecto Tor a una computadora donde puedas guardar archivos. Inserta tu unidad USB y copia el paquete del Navegador Tor a esta unidad. Usando esta unidad USB y cualquier computadora con Windows donde puedas insertar un disco USB, puedes acceder a un navegador protegido por Tor. En esta computadora compartida, cierra el navegador web existente. Inserta el disco, encuentra los archivos de este disco en el Escritorio, y haz doble clic sobre Start Tor Browser.exe. La ventana de Vidalia aparecerá en breve.

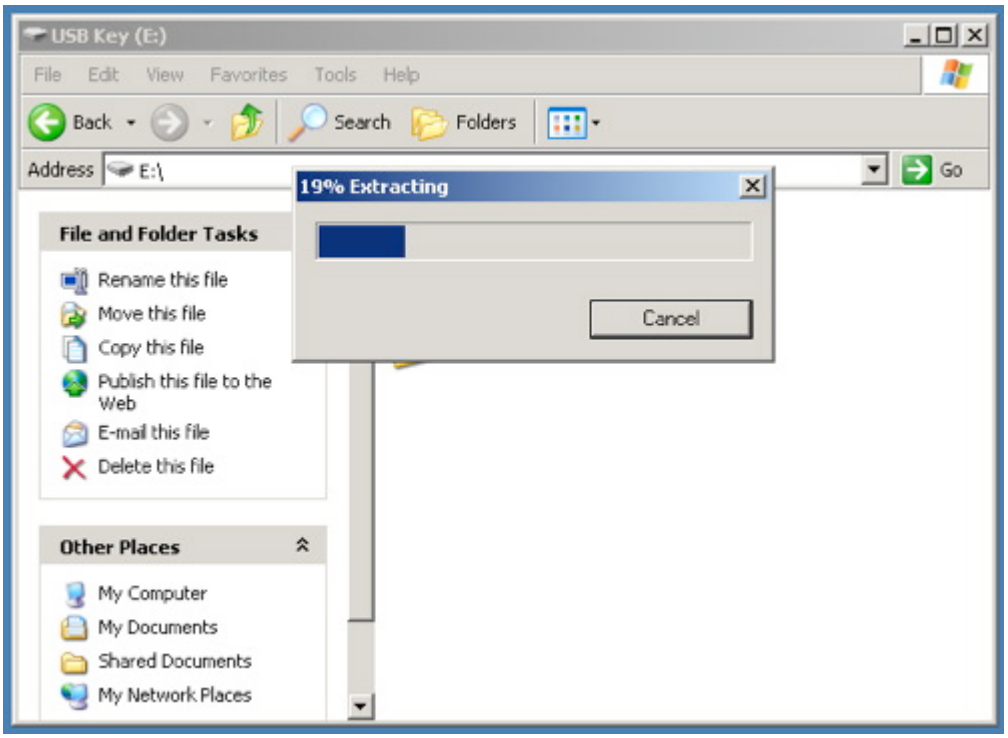


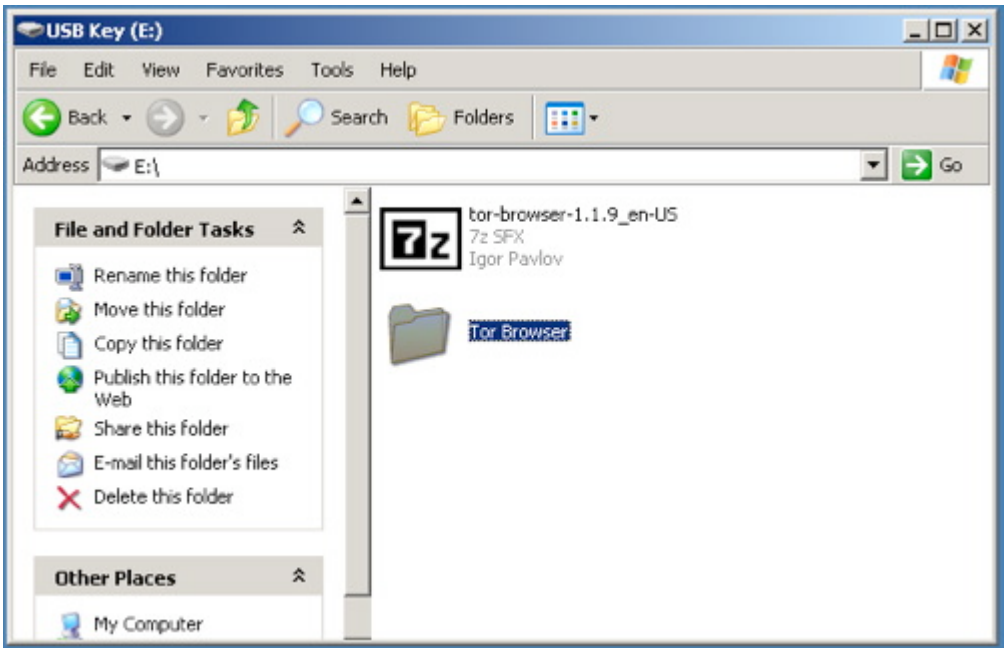
Recuerda que puedes descargar el Tor Browser Bundle desde el sitio web del Proyecto Tor o elegir el paquete de tu idioma preferido desde la página de descarga del Tor Browser Bundle.

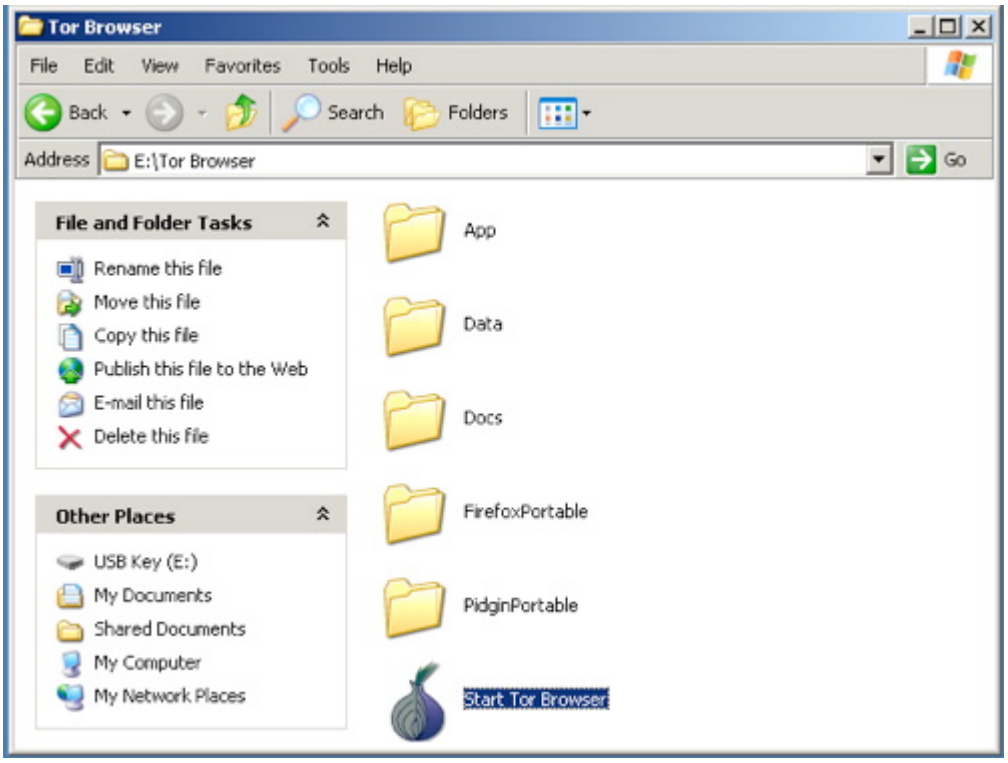

Tor Browser Bundle - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.torproject.org/torbrowser/index.html.en#Extraction
Most Visited Getting Started Latest Headlines
If you have an unreliable Internet connection, it may be easier for you to download the bundle edition which is split up into smaller parts.
Tor Browser Bundle for Windows with Firefox (version 1.1.9, 15 MB)
Opening tor-browser-1.1.9_en-US.exe
You have chosen to open
tor-browser-1.1.9_en-US.exe
which is a: Application
from: https://www.torproject.org
Would you like to save this file?
Save File
Cancel
English
Deutsch
Español
Français
Nederla
Português (pt-PT) (signature)
Русский (ru) (signature)
(zh-CN) (signature)

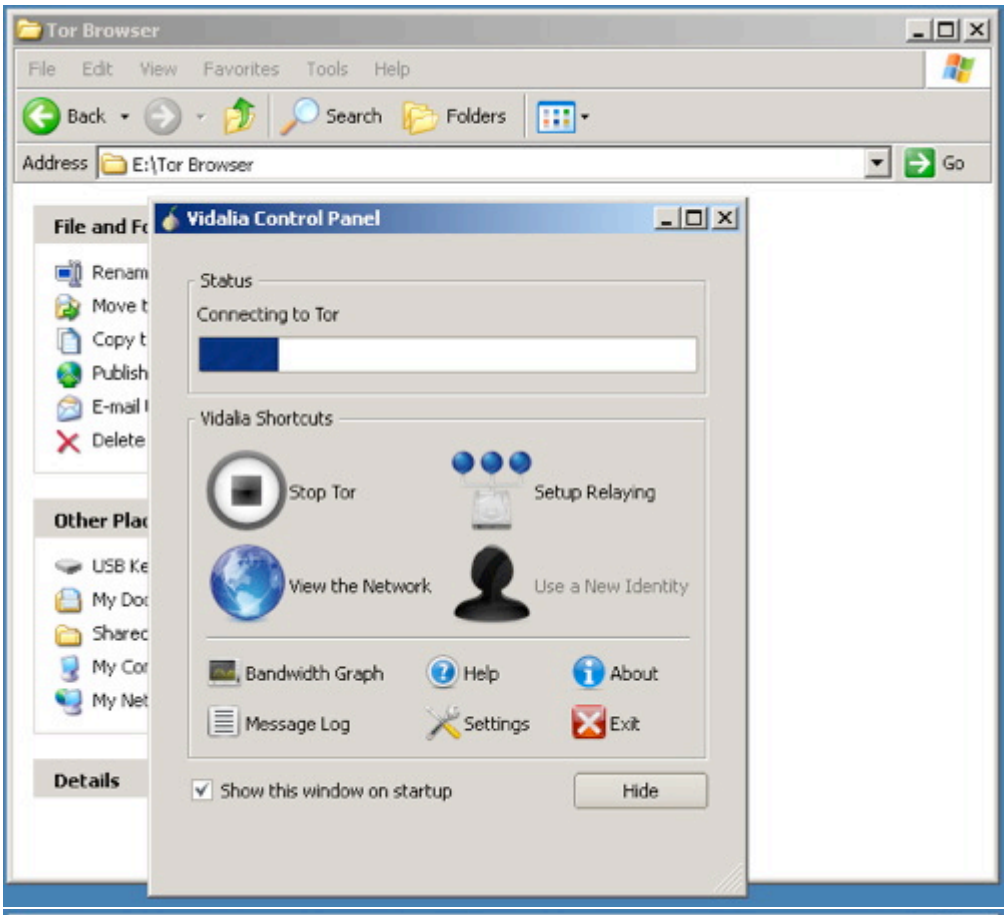

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
My Computer
My Documents
Shared Documents
My Network Places
Details
tor-browser-1.1.9_en-US
7z SFX
Igor Pavlov
My Network Places
Recycle Bin
Internet Explorer
Mozilla Firefox
Parallels Shared Folders
Start
USB Key (E:)

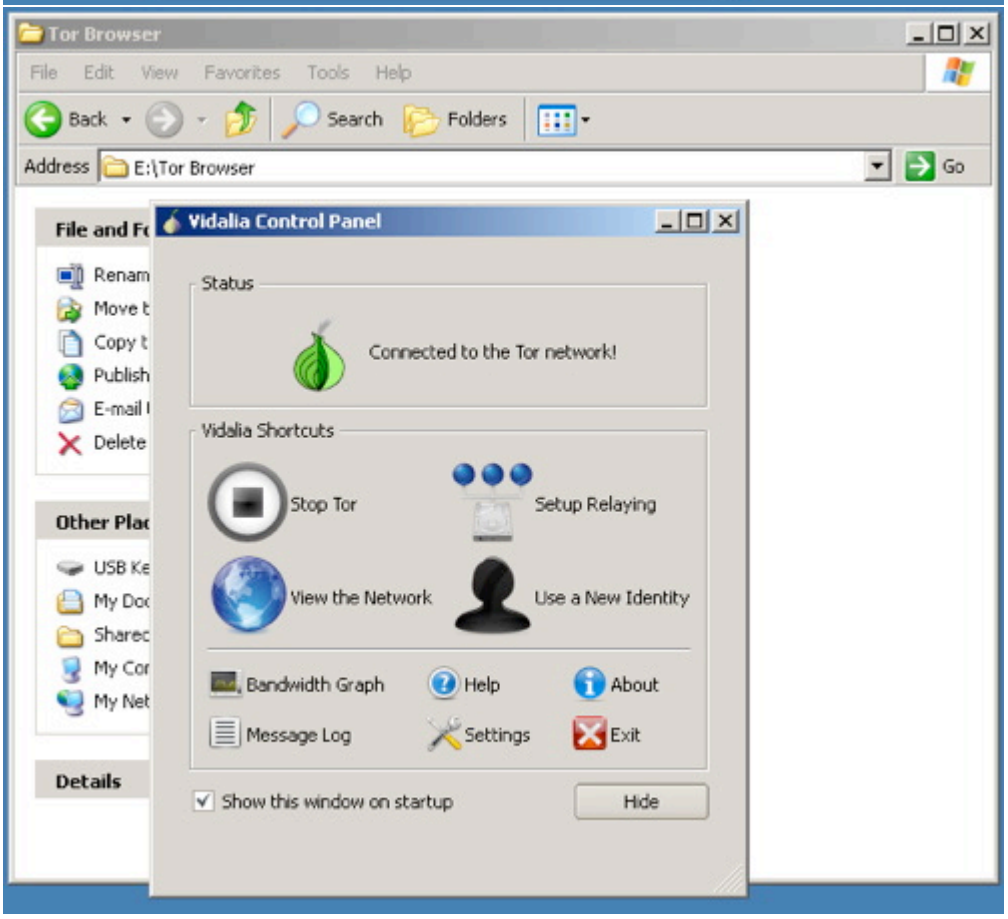

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share t
Other Plac
My Cor
My Doc
Shared
My Network Places
Details
tor-browser-1.1.9_en-US
7z SFX
Igor Pavlov
7-Zip self-extracting archive
Extract to:
E:\
...
Extract
Cancel

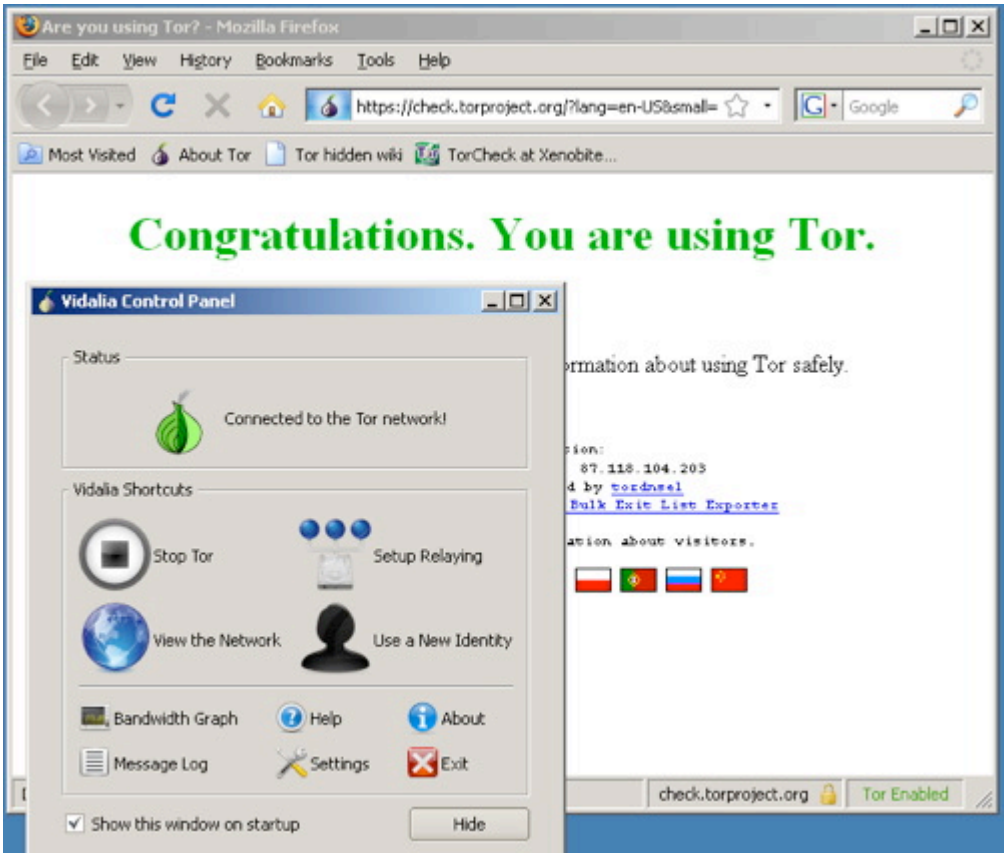

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
19% Extracting
Cancel
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
My Computer
My Documents
Shared Documents
My Network Places


USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
File and Folder Tasks
Rename this folder
Move this folder
Copy this folder
Publish this folder to the Web
Share this folder
E-mail this folder's files
Delete this folder
Other Places
My Computer
tor-browser-1.1.9_en-US
7z SFX
Igor Pavlov
Tor Browser


Tor Browser
File Edit View Favorites Tools Help
Back Search Folders
Address E:\Tor Browser
Go
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
USB Key (E:)
My Documents
Shared Documents
My Computer
My Network Places
App
Data
Docs
FirefoxPortable
PidginPortable
Start Tor Browser


Tor Browser
File Edit View Favorites Tools Help
Back Search Folders
Address E:\Tor Browser
Go
Vidalia Control Panel
Status
Connecting to Tor
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide
Details


Tor Browser
File Edit View Favorites Tools Help
Back Search Folders
Address E:\Tor Browser
Go
Vidalia Control Panel
Status
Connected to the Tor network!
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide
Details



b) Extrae el archivo en tu unidad USB, abre la carpeta "Tor Browser" y haz clic en "Start Tor Browser". Después de conectar a la red de Tor, el navegador Firefox habilitado con Tor comenzará automáticamente por visitar el sitio de prueba de Tor. Asegúrate de que obtienes un mensaje de "Felicidades. Estás usando Tor".
De lo contrario, obtendrás un mensaje diciéndote "Lo siento. No estás usando Tor. Si estás intentando usar un cliente Tor, por favor dirígete al sitio web de Tor y específicamente, a las instrucciones para configurar tu cliente Tor".

II – Escribir desde tu computadora personal.

Ahora bien, si vas a bloguear principalmente desde tu computadora personal, en la cual puedes instalar software, por favor sigue los pasos indicados a continuación.

Paso 1: Enmascara tu IP.

Cada computadora en Internet tiene o comparte una dirección IP. Estas direcciones no son lo mismo que una dirección física, pero pueden guiar a un administrador de sistemas listo hasta tu dirección física. En particular, si trabajas para un ISP, a menudo puedes asociar una dirección IP con el número telefónico que requirió esa IP en un momento específico. Así que, antes de que hagamos nada anónimo en internet, necesitamos enmascarar nuestra IP.
Qué hacer si quieres bloguear desde la computadora de tu casa o trabajo:

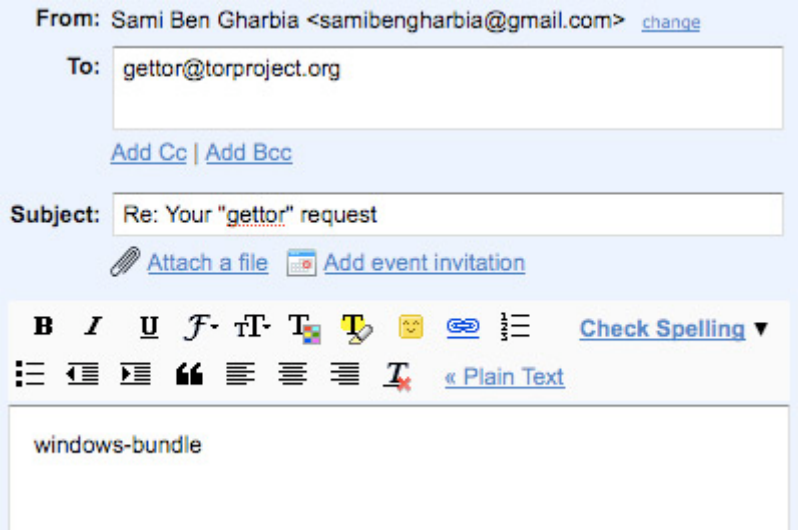
a) **Instala Firefox.** Descárgalo en el sitio web de Mozilla e instálalo en la máquina desde la cual escribes.

¿Por qué?
Internet Explorer tiene algunos agujeros de seguridad graves que pueden comprometer tu seguridad en línea. Estos agujeros tienden a mantenerse sin parchar por más tiempo en IE que en otros navegadores. (¿No me crees? Pregúntale a Bruce Schneier.) Es el navegador más vulnerable a spyware que podrías descargar inadvertidamente desde un sitio web. Y muchas de las herramientas de privacidad siendo liberadas están siendo escritas para funcionar específicamente en Firefox, incluyendo Torbutton, el cual estaremos empleando en un paso futuro.

b) Instala Tor. Descarga el programa desde el sitio web de Tor. Si el acceso al sitio web principal de Tor está bloqueado en tu país, existen algunos espejos de éste en otros lugares donde también puede ser descargado. También puedes ir al caché de Google para ver los sitios espejo, googleando "site:torproject.org mirrors". Elige la "última versión estable" para tu plataforma y descárgala a tu escritorio. Sigue las instrucciones que se encuentran a la derecha de la versión que elegiste. Instalarás dos paquetes de software y necesitarás hacer algunos cambios en la configuración de tu nueva instalación de Firefox.

En caso de que tu conexión a Internet bloquee el acceso al sitio web de Tor, puedes solicitar el paquete, enviando un email al robot "gettor", a *gettor [AT] torproject [DOT] org*. Recuerda que los emails enviados a gettor@torproject.org tienen que venir de Gmail, de lo contrario no obtendrán respuesta. Elige uno de los siguientes nombres de paquete y ponlo en cualquier sitio, en el cuerpo de tu email:

- tor-im-browser-bundle
- windows-bundle
- panther-bundle
- tor-browser-bundle
- source-bundle
- tiger-bundle



Poco después de enviar tu email, recibirás un email del robot "Gettor" con el software requerido como un archivo comprimido (zip). Descomprime el archivo y verifica la firma.

gettor@torproject.org to me

Hello! This is the "gettor" robot.

Here's your requested software as a zip file. Please unzip the package and verify the signature.

Hint: If your computer has GnuPG installed, use the gpg commandline tool as follows after unpacking the zip file:

gpg --verify <packagename>.asc <packagename>

The output should look somewhat like this:

gpg: Good signature from "Roger Dingledine <arma@mit.edu>"

If you're not familiar with commandline tools, try looking for a graphical user interface for GnuPG on this website:

http://www.gnupg.org/related_software/frontends.html

If your internet connection blocks access to the Tor network, please consider using a bridge relay. Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

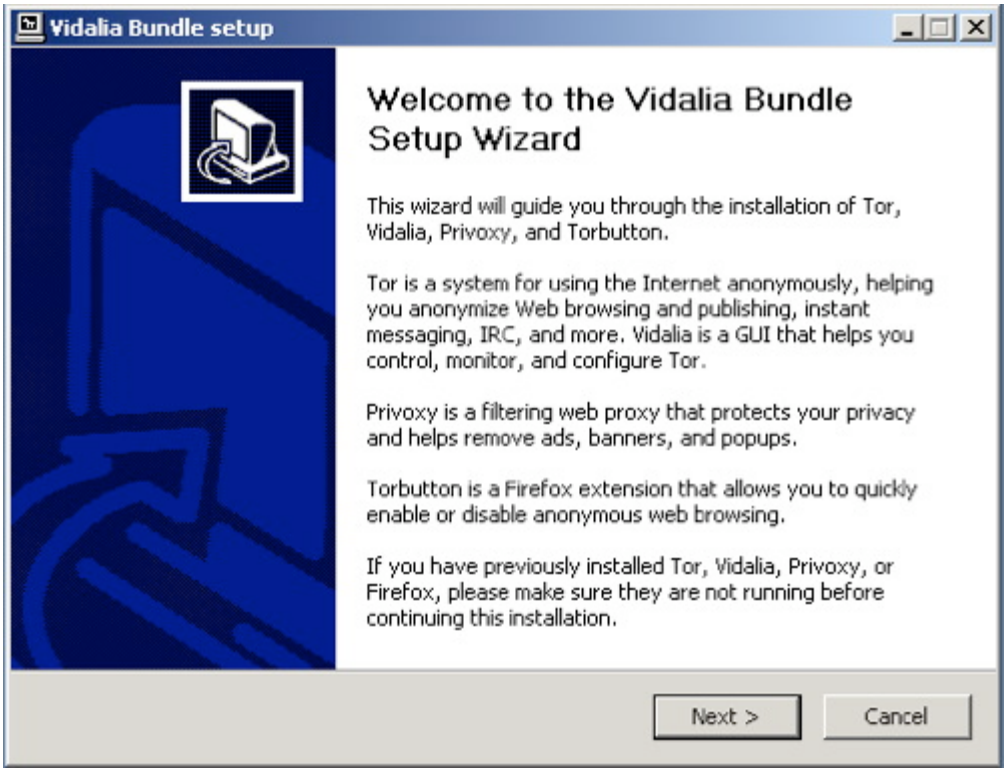
You can acquire a bridge by sending an email that contains "get bridges" in the body of the email to the following email address: bridges@torproject.org

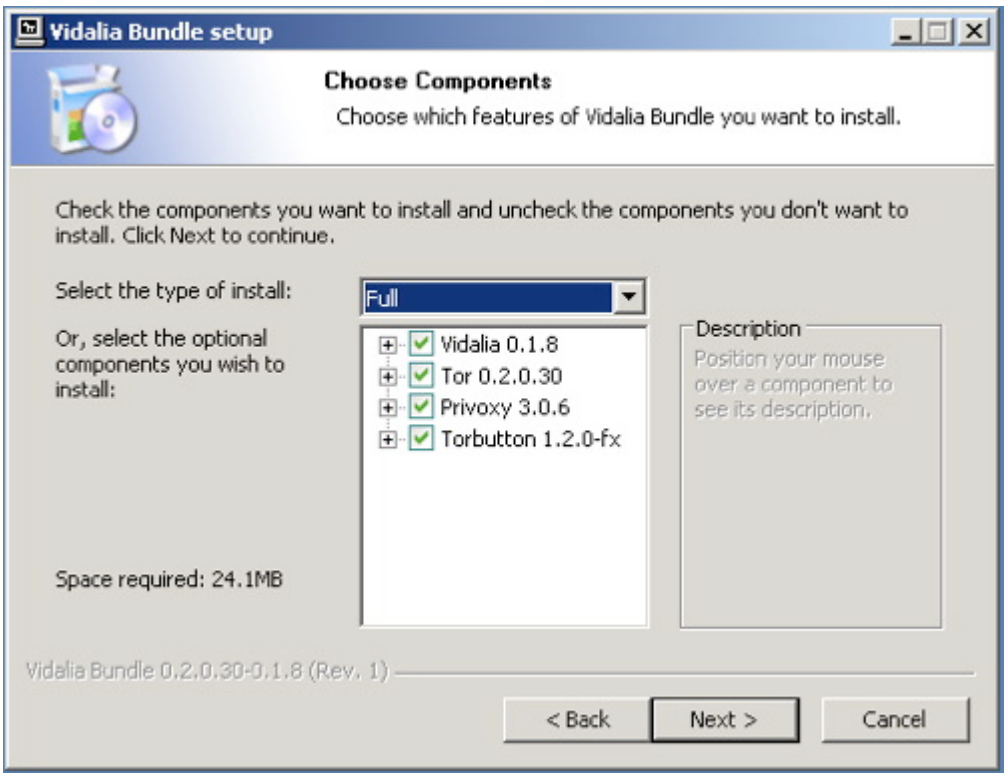
It is also possible to fetch bridges with a web browser at the following url: https://bridges.torproject.org/

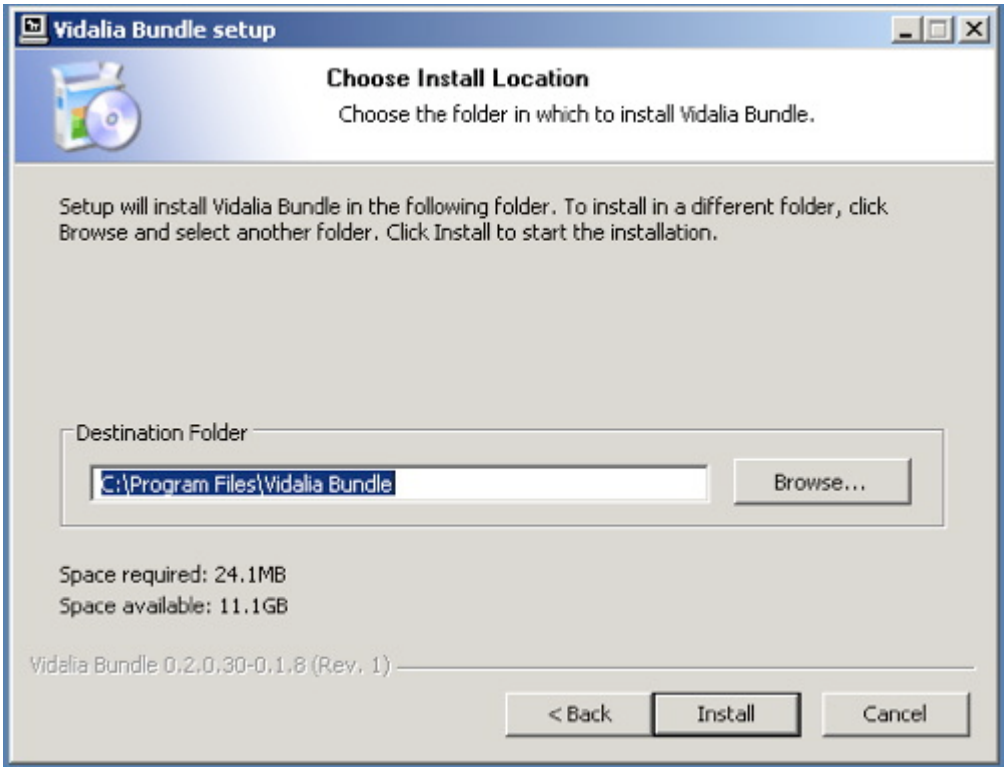
- Show quoted text -

Oops... the virus scanner has a problem right now. Download at your own risk, or try again later.

windows-bundle.z
8219K Download


Vidalia Bundle setup
Welcome to the Vidalia Bundle Setup Wizard
This wizard will guide you through the installation of Tor, Vidalia, Privoxy, and Torbutton.
Tor is a system for using the Internet anonymously, helping you anonymize Web browsing and publishing, instant messaging, IRC, and more. Vidalia is a GUI that helps you control, monitor, and configure Tor.
Privoxy is a filtering web proxy that protects your privacy and helps remove ads, banners, and popups.
Torbutton is a Firefox extension that allows you to quickly enable or disable anonymous web browsing.
If you have previously installed Tor, Vidalia, Privoxy, or Firefox, please make sure they are not running before continuing this installation.
Next >
Cancel

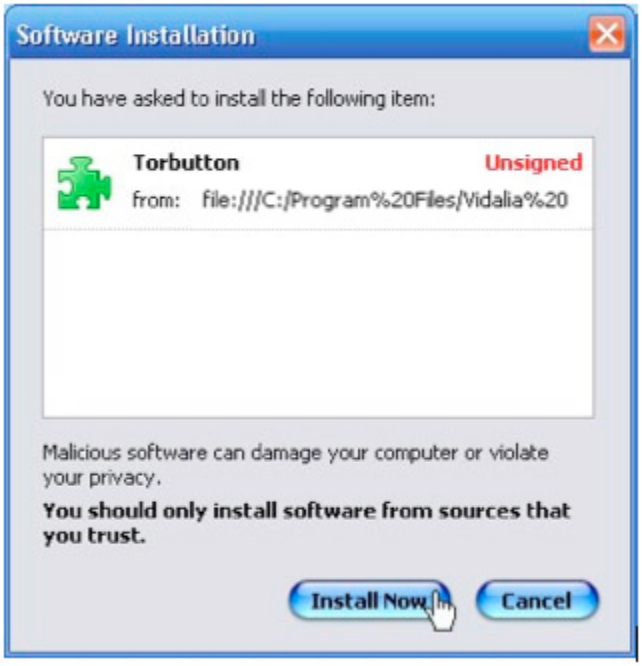

Vidalia Bundle setup
Choose Components
Choose which features of Vidalia Bundle you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Full
Or, select the optional components you wish to install:
Vidalia 0.1.8
Tor 0.2.0.30
Privoxy 3.0.6
Torbutton 1.2.0-fx
Description
Position your mouse over a component to see its description.
Space required: 24.1MB
Vidalia Bundle 0.2.0.30-0.1.8 (Rev. 1)
< Back
Next >
Cancel



¿Por qué?
Tor es una red muy sofisticada de servidores proxy. Los servidores proxy solicitan una página en tu nombre, lo que significa que el servidor web no ve la dirección IP de la computadora que está solicitando la página web. Cuando accedes a Tor, estás usando tres servidores web diferentes para obtener cada página web. Las páginas están encriptadas en su tránsito entre servidores, y aún si uno o dos de los servidores en la cadena se ven comprometidos, sería muy difícil ver cuál página web estabas recuperando o publicando.

Tor instala otra pieza de software, Privoxy, lo cual incrementa la configuración de seguridad en tu navegador, bloqueando cookies y otros tipos de software de seguimiento. Convenientemente, también bloquea muchos anuncios que encuentras en páginas web.

c) El paquete también instala el plugin de Firefox Torbutton para ti. Éste simplemente solicitará tu permiso para instalarse desde el paquete descargado. Haz clic en "Instalar ahora", reinicia tu Firefox, y estás listo:



¿Por qué?
Iniciar Tor manualmente significa recordar cambiar las preferencias de tu navegador para usar un servidor proxy. Este es un proceso de pasos múltiples, lo que significa que la gente a menudo olvida hacerlo. Torbutton convierte el proceso en un solo clic de ratón, y te recuerda si estás usando Tor o no, lo que puede ser muy útil.

Puedes encontrar que Tor ralentiza tu uso de la web –esto es resultado del hecho de que las solicitudes hechas a través de Tor se enrutan a través de tres proxies antes de alcanzar el servidor. Algunas personas –incluyéndome- usan Tor solo en situaciones en las que es importante disfrazar la identidad, y lo desconectan si no –el botón Tor hace esto muy fácil.

d) Conecta Tor en Firefox y pruébalo. Con Tor activado, visita esta URL(https://check.torproject.org/). Luego de hacer clic, si recibes un mensaje que te indica, "Felicidades. Estás usando Tor. Por favor dirígete al sitio web de Tor para mayor información acerca de usar Tor de manera segura", entonces tienes todo instalado correctamente y estás listo para el siguiente paso.

De lo contrario obtendrás este mensaje diciéndote "Lo siento. No estás usando Tor. Si estás intentando usar un cliente de Tor, por favor dirígete al sitio web de Tor y específicamente a las instrucciones para configurar tu cliente de Tor."

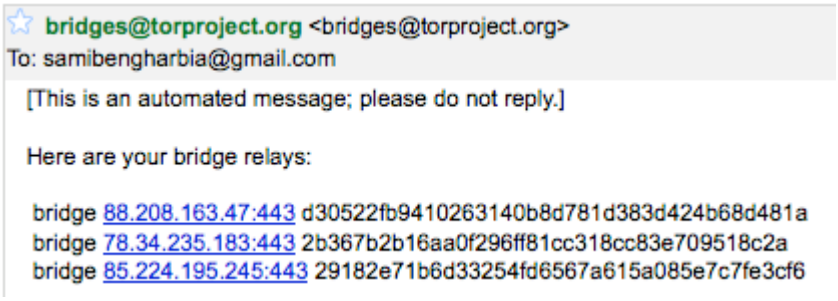
¿Por qué?
Es siempre una buena idea comprobar si el software que has instalado funciona, especialmente cuando está haciendo algo tan importante como lo que hace Tor. La página a la que estás accediendo está comprobando desde cuál dirección IP proviene tu solicitud. Si es desde un nodo Tor conocido, Tor está funcionando correctamente y tu dirección IP está enmascarada –si no, algo está mal y deberías tratar de averiguar por qué Tor no está funcionando correctamente.

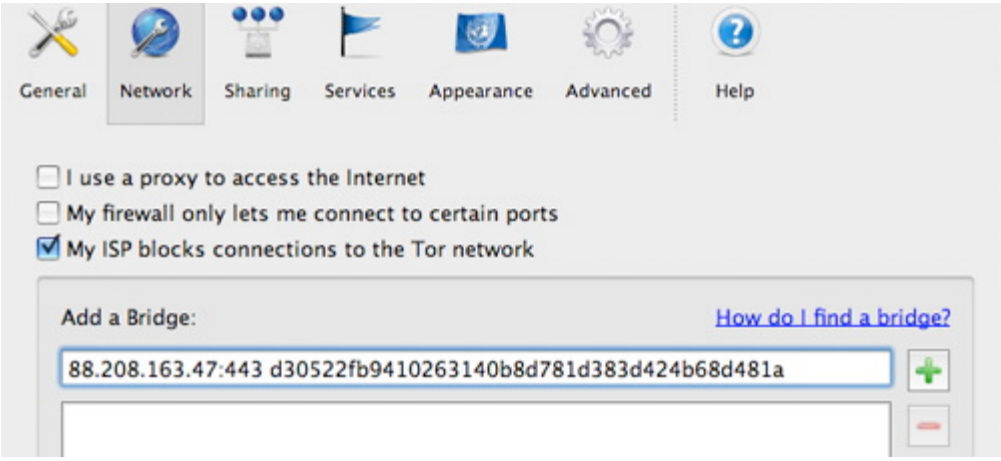
¿Qué si Tor nunca se conecta?
Si tienes problemas conectándote a la red de Tor, deberías leer las preguntas frecuentes acerca de problemas relacionados con correr Tor adecuadamente. En caso de que tu conexión a Internet bloquee el acceso a la red de Tor y en caso de que el icono de cebolla de Vidalia en la bandeja de sistema sea siempre amarillo, puedes considerar usar puentes. Éste sería el siguiente paso lógico para hacer que puedas conectarte a la red de Tor.

"*Los puentes de retransmisión (o simplemente "puentes") son retransmisores usados por Tor que no están listados en el directorio principal de Tor. Ya que no existe una lista pública completa de ellos, aún en el caso de que tu ISP esté filtrando conexiones a todos los retransmisores de Tor conocidos, probablemente no serán capaces de bloquear todos los puentes. Si sospechas que tu acceso a la red de Tor está siendo bloqueado, quizás quieras usar la configuración de puentes de Tor."*

Puedes obtener puentes enviando un email que contenga "get bridges" en el cuerpo del email, desde una cuenta gmail, a la dirección electrónica bridges@torproject.org. Poco tiempo después, recibirás un mensaje automático con los puentes. También es posible obtener puentes en la siguiente dirección url: https://bridges.torproject.org/

Abre el Panel de Control de Vidalia, ve a Configuración > Red y haz clic en "Mi ISP bloquea conexiones a la red Tor". Añade cada dirección de Puente, una a la vez, copiándola y pegándola en la ventana "Agregar un puente" y luego haciendo clic en el signo de "+".





Paso 2: Genera una nueva dirección de correo electrónico, difícil de rastrear.

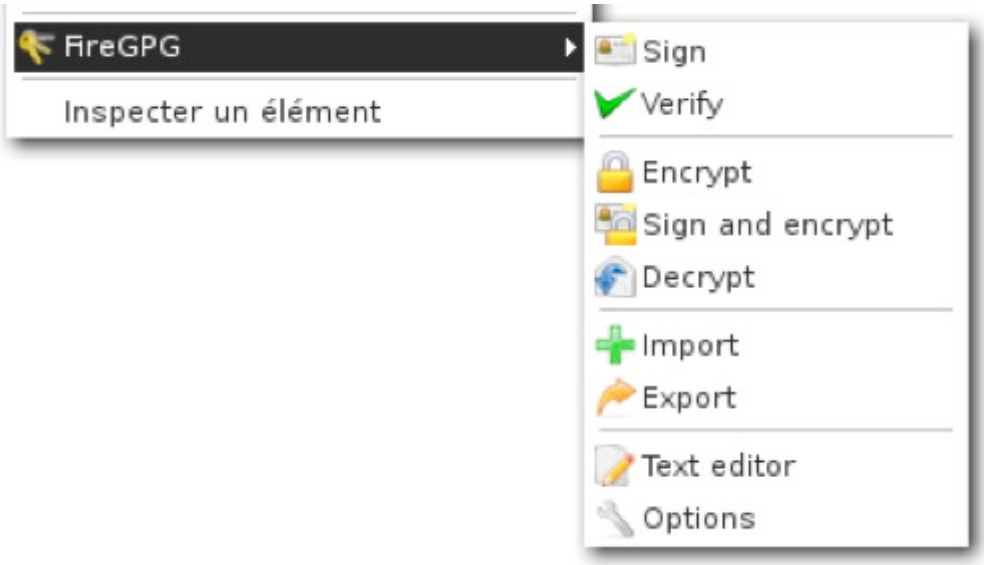
La mayoría de los servicios web –incluyendo los servicios de hospedaje de blogs-requieren una dirección de correo electrónico para comunicarse con sus usuarios. Para nuestros propósitos, esta dirección no puede conectarse con ninguna información personalmente identificable, incluyendo la dirección IP que utilizamos para inscribirnos en el servicio. Esto significa que necesitamos una nueva cuenta para la cual nos inscribiremos usando Tor, y necesitamos asegurarnos que ninguno de los datos que usamos –nombre, dirección, etcétera- puede ser vinculado con nosotros. Tú NO debes usar una dirección de correo electrónico previamente existente. –Es muy probable que te registraras para esa cuenta desde una dirección IP no enmascarada, y la mayoría de los proveedores de correo electrónico almacenan la dirección IP desde la cual te registraste.

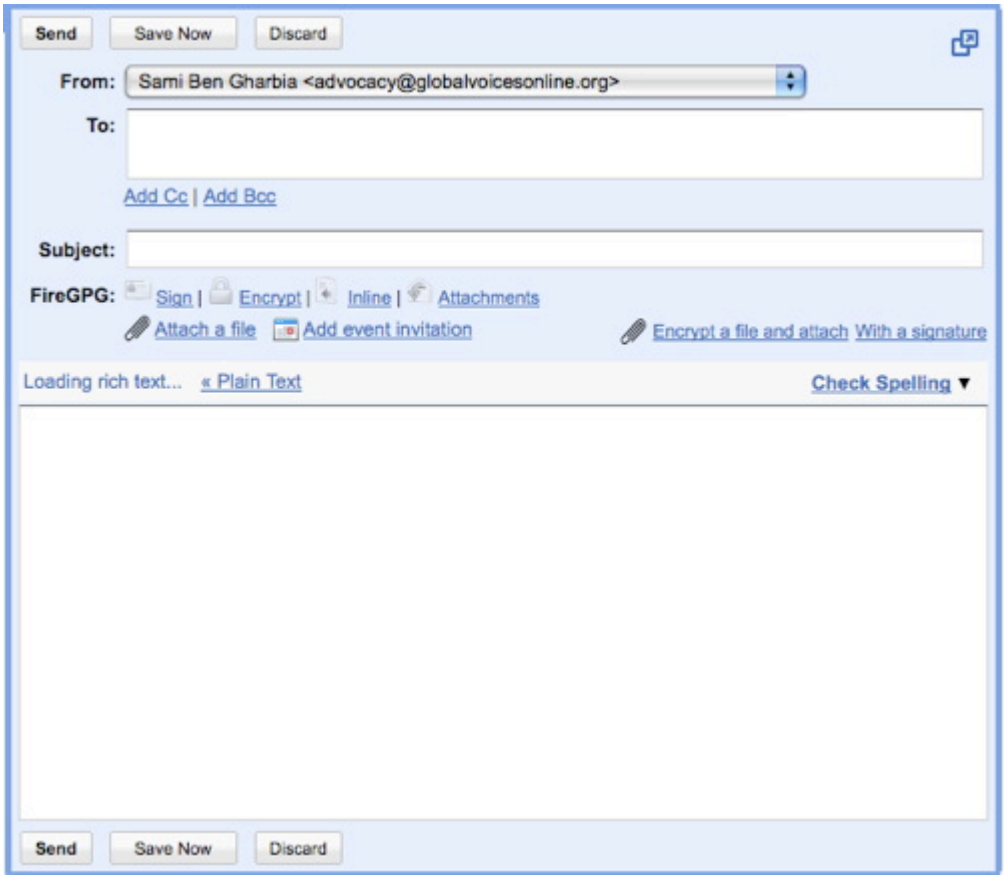
a) Elige un proveedor de correo electrónico – Nosotros recomendamos Riseup.net y Gmail, pero siempre y cuando estés usando Tor, podrías perfectamente emplear Yahoo o Hotmail. También puedes registrar fácilmente una cuenta rápida y gratuita con fastmail.fm.

¿Por qué?

El correo electrónico web es la mejor manera de crear una dirección de e-mail "desechable", una que puedes usar para inscribirte en diversos servicios e ignorar el resto del tiempo. Pero muchos usuarios también usan el correo electrónico web como su email principal. Si tú haces esto, es importante entender algunas de las fortalezas y debilidades de los diferentes proveedores de correo electrónico. Tanto Hotmail como Yahoo tienen una "característica de seguridad" que hace a los defensores de la seguridad muy infelices. Ambas incluyen la dirección IP de la computadora empleada para enviar cualquier email. Esto no es relevante cuando estás accediendo a esos servicios a través de Tor, puesto que la dirección IP será una dirección IP de Tor, en lugar de la tuya. Asimismo, Hotmail y Yahoo no ofrecen interfaces HTTP seguras (https) para su correo electrónico web –de nuevo, esto no importa siempre y cuando uses Tor cada vez que empleas estos servicios de correo. Pero muchos usuarios querrán revisar su correo en circunstancias en las cuales no tengan Tor instalado –para tu dirección de correo principal, vale la pena elegir un proveedor que tenga una interfaz https para el correo.

Riseup.net provee correo electrónico con un alto nivel de seguridad. Soportan encriptado PGP (Pretty Good Privacy) el cual es muy útil si intercambias correspondencia con personas que también usen PGP. Puedes registrar una cuenta gratuita en www.riseup.net y pedirle a las personas que intercambian correspondencia contigo que registren una cuenta gratuita también.
Gmail, aún cuando no se publicita a sí mismo como un servicio de correo electrónico seguro, tiene algunas características de seguridad incorporadas. Si visitas esta URL especial (https://mail.google.com/mail), toda tu sesión de Gmail será encriptada vía https. También puedes visitar https://mail.google.com/mail/h/ una dirección SSL de Gmail que carga automáticamente en la interfaz de HTML básico. (Yo recomiendo crear un marcador de esa URL y usarla para todas tus sesiones de Gmail). Gmail no incluye la IP de origen en las cabeceras de los correos, y puedes añadir soporte PGP empleando el FireGPG, una extensión de Firefox que añade un fuerte encriptado a Gmail. FireGPG trae una interfaz para encriptar, desencriptar, firmar o verificar la firma del texto en cualquier página web que esté empleando GnuPG.





Una advertencia en cuanto a todas las cuentas de correo electrónico web –estás confiando en la compañía que provee el servicio, todo tu correo electrónico. Si esa compañía es hackeada, o si son presionados por otros gobiernos para revelar información, ellos tendrán acceso al texto de todos los correos que has recibido y enviado. La única manera de sortear esto es escribir tus correos en un editor de texto, encriptarlos en tu propia máquina usando PGP y enviarlos a alguien que también esté usando PGP. Esto va mucho más allá del nivel de secreto que la mayoría de nosotros queremos y necesitamos, pero es importante recordar que estás confiando en a una compañía que podría o no querer tus mejores intereses. Yahoo, en específico, tiene un desagradable hábito de entregar información al Gobierno de China –los disidentes chinos están ahora demandando a la compañía por liberación ilegal de sus datos. Sólo algo en lo que pensar cuando decidas en quién confiar…

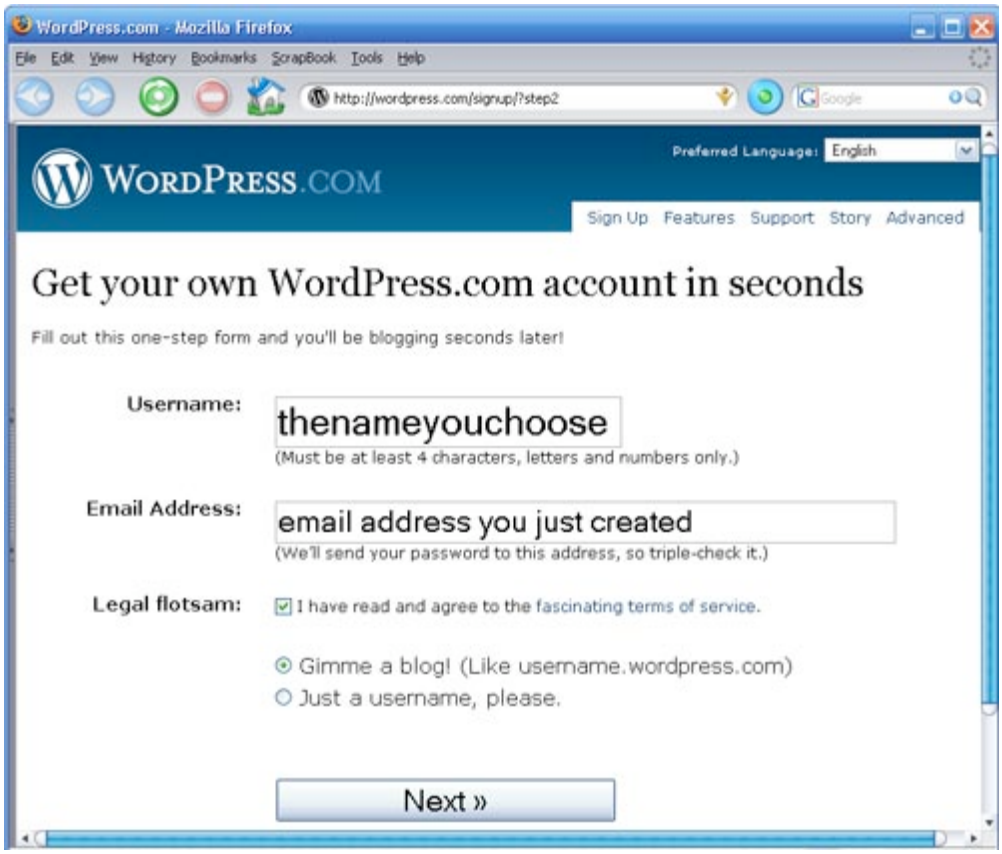
b) Activa Tor en tu navegador, o inicia el Tor Browser desde tu disco USB. Visita el sitio de correo electrónico que hayas elegido, y registra una nueva cuenta. No uses ninguna información personalmente identificable –considera convertirte en un individuo de nombre aburrido en un país con muchos usuarios de internet, como los EEUU o el Reino Unido. Crea una contraseña buena y fuerte (al menos ocho caracteres, incluyendo al menos un número o un carácter especial) para la cuenta, y elige un nombre de usuario similar al nombre que vas a darle a tu blog.

c) Asegúrate de que puedes iniciar sesión en el servicio de correo y enviar correo cuando Tor está habilitado. Lo más probable es que Tor cambie su circuito cada diez minutos, y esto podría interrumpir tus operaciones en tu correo electrónico, así que deberías considerar limitar el proceso de escribir un nuevo email a diez minutos.

Paso 3: Registra tu nuevo blog anónimo.

a) Activa Tor en tu navegador, o inicia el Tor Browser Bundle. **Visita Wordpress.com y registra una nueva cuenta** haciendo clic en el link "Obtén un nuevo Blog de Wordpress". Usa la dirección de

email que acabas de crear y crea un nombre de usuario que sea parte de la dirección de tu blog: elnombrequeelegiste.wordpress.com



b) Wordpress te enviará un link de activación a tu cuenta de correo. Usa tu navegador habilitado con Tor para encontrar ese correo electrónico, y **sigue el vínculo de activación.** Esto permite a Wordpress saber que has usado una cuenta de correo activa y que pueden enviarte actualizaciones sobre el servicio –como resultado de esto, harán tu blog públicamente visible y te enviarán tu contraseña. Necesitarás revisar tu buzón de nuevo para encontrar esta contraseña.

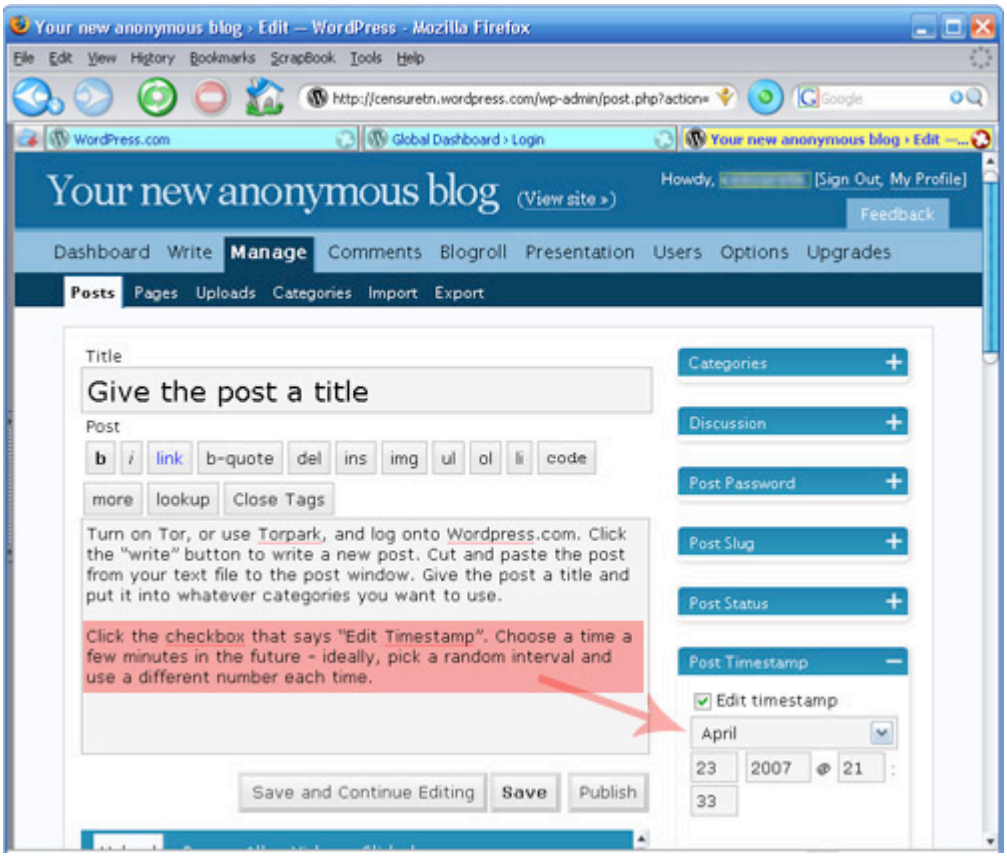
c) Aún usando Tor, accede a tu nuevo blog usando tu nombre de usuario y contraseña. Haz clic en "Escritorio" y luego en "Usuarios > Opciones personales > Detalles de cuenta". **Cambia tu contraseña** a una contraseña fuerte, que puedas recordar. Siéntete libre de añadir información a tu perfil, también… ¡sólo asegúrate de que ninguno de esos datos esté relacionado contigo!

Paso 4: Publica en tu blog.

a) Escribe tu artículo fuera de línea. No sólo es una buena manera de evitar perder un post si tu navegador falla o tu conexión se cae, también significa que puedes redactar tus posts en un lugar más privado que en un cibercafé. Un simple editor de texto, como Wordpad para Windows, es usualmente lo mejor. Guarda tus artículos como archivos de texto (después de bloguear, siempre recuerda remover estos archivos de tu máquina por completo, usando una herramienta como Eraser o Ccleaner, la cual está disponible en muchos idiomas y borra archivos temporales automáticamente de todos los navegadores instalados y de otras aplicaciones.

b) Activa Tor, o usa Tor Browser desde tu disco portátil, e inicia sesión en Wordpress.com. Haz clic en el botón de "Escribir" para escribir un nuevo post. Copia y pega el post desde tu archivo de texto a

la ventana de publicación. Dale un título al post y ubícalo en cualesquiera categorías que quieras emplear.
Antes de que presiones "Publicar", hay un paso clave. Haz clic en la barra azul a la derecha de la pantalla que dice "Fecha y hora". Haz clic en la casilla de verificación que dice "Editar Fecha y Hora". Elige una hora que esté algunos minutos en el futuro –idealmente, elige un intervalo aleatorio y usa un número diferente cada vez. Esto pondrá un retraso variable en el tiempo en el que tu artículo aparecerá en el sitio –Wordpress no pondrá el post hasta que llegue el momento que has especificado.

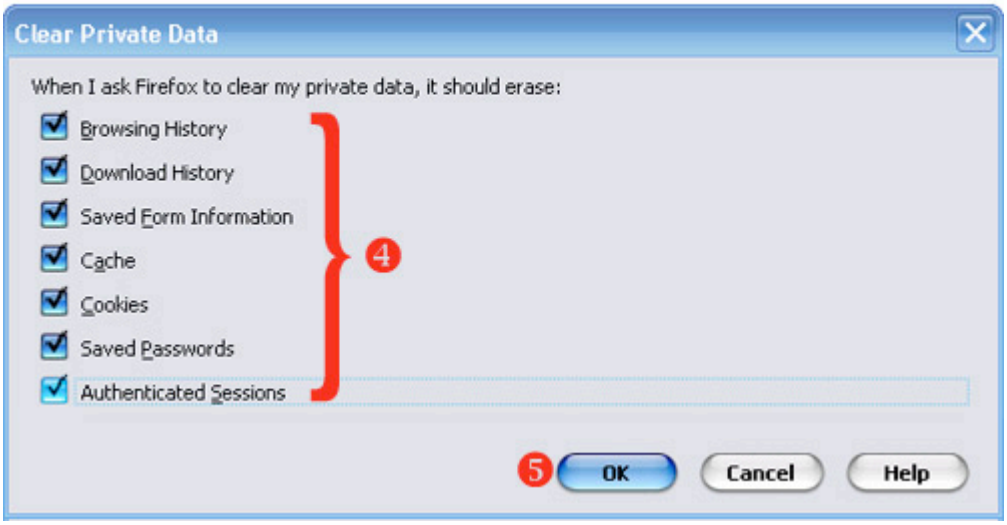


¿Por qué?

Al editar la fecha y hora, estamos protegiéndonos contra una técnica que alguien podría usar para tratar de determinar tu identidad. Imagina que estás escribiendo un blog llamado "¡Abajo la Compañía de Telecomunicaciones de Etiopía!" Alguien en la CTE podría comenzar a seguir ese blog de cerca y preguntarse si uno de sus clientes está escribiendo el blog. Comenzarían a registrar las veces que un post fue publicado en abajolacte.wordpress.com, y comparar estas marcas de fecha y hora contra sus registros de uso. Descubrirían que unos pocos segundos antes de que cada post fuera publicado, durante el tiempo de un mes, uno de sus clientes estaba accediendo a uno u otro nodo de Tor. Podrían entonces concluir que este usuario está empleando Tor para publicar en el blog, y entregarían esta información a la policía.
Al cambiar la fecha y hora de los post, hacemos este ataque más difícil para el ISP. Ahora necesitarán también acceso a los registros del servidor de Wordpress, lo que será mucho más difícil de conseguir que los suyos. Es un paso muy simple que incrementa tu seguridad.

Paso 5: Cubre tus huellas.

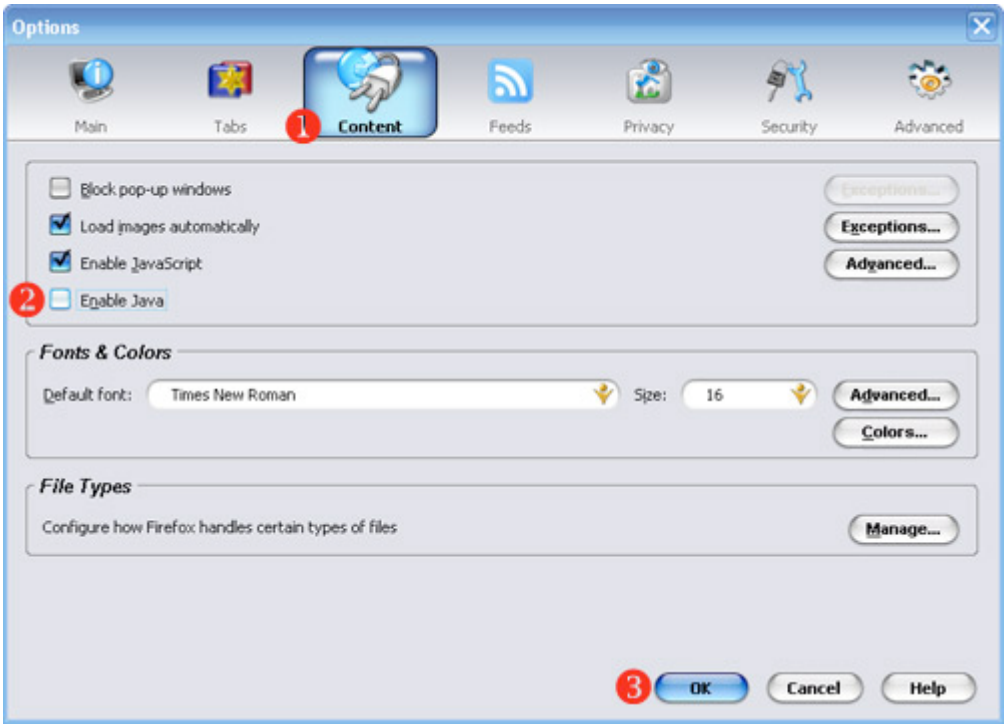
a) Borra de manera segura los borradores de los artículos que has escrito desde tu laptop o la computadora de tu casa. Si empleaste un disco USB para llevar el post al cibercafé, necesitarás borrar éste, también. No es suficiente con mover el archivo a la papelera de reciclaje y vaciar la papelera – necesitas emplear una herramienta de borrado seguro, como Eraser o Ccleaner, las cuales sobrescriben los viejos archivos con data que los hace imposible de recuperar. En una Macintosh, esta funcionalidad está incorporada –lleva un archive a la papelera y elige "Vaciado seguro de la papelera" desde el Menú del Finder.
b) Limpia tu historial de navegación, cookies y contraseñas de Firefox. Bajo el menu Herramientas, selecciona "Limpiar información privada". Marca todas las casillas y haz clic en "Aceptar". Puedes querer configurar Firefox de modo que automáticamente limpie todos tus datos cada vez que cierras – puedes hacer esto en "Firefox -> Preferencias -> Privacidad -> Configuración". Elige la casilla que dice "Limpiar datos privados cuando se cierre Firefox". En caso de que no puedas instalar programas en la computadora, usa la herramienta IE Privacy Cleaner desde el disco USB para limpiar información temporal de navegación.



¿Por qué?
Es muy fácil para alguien ver los sitios web que has visitado en una computadora, solo revisando el historial de tu navegador. Fisgones más sofisticados pueden hallar tu historial de búsquedas revisando los archives de tu caché, lo que incluye versiones almacenadas de páginas web. Queremos limpiar toda esta data de nuestra computadora personal, para que el siguiente usuario no la encuentre. Y queremos eliminarla de nuestra computadora personal, para que, si esa computadora se pierde, es robada o confiscada, no podamos ser relacionados con los posts que hemos escrito.
Algunos pensamientos finales:
- No es suficiente protegerte a ti mismo solo cuando estás escribiendo en tu propio blog. Si vas a publicar comentarios en otros blogs usando tu seudónimo, necesitarás usar Tor cuando publiques esos comentarios también. La mayoría del software de los blogs registra la IP desde la cual vino un comentario – si no usas Tor, estás invitando a quien sea que administra ese sitio a rastrear tu dirección de IP hasta tu computadora. Tor es como un condón –no practiques blogging inseguro.

- Sólo porque eres anónimo no significa que no debas hacer tu blog bonito. La pestaña de "Apariencia" en Wordpress tiene muchas opciones con las cuales jugar –puedes elegir distintas plantillas, incluso subir fotos para personalizar algunas de ellas. Pero sé muy, muy cuidadoso al usar tus propias fotos – proporcionas un montón de información acerca de ti mismo al publicar una foto (si la foto fue tomada en Zambia, por ejemplo, es evidencia de que estás o estuviste en Zambia).

- Si estás realmente preocupado acerca de tu seguridad, quizás quieras ir un paso más allá y configurar tu navegador Firefox para desactivar Java. Hay un desagradable bache de seguridad en la versión más reciente de Java, que permite al autor de un script malicioso averiguar qué IP se le ha asignado a tu computadora INCLUSO SI ESTÁS USANDO TOR. Nosotros no nos preocupamos mucho acerca de esto, porque no creemos que Wordpress.com o Google estén corriendo estos scripts maliciosos… pero es algo para considerar seriamente si estás usando Tor por otras razones. Para desactivar Java, ve a "Firefox -> Preferencias -> Contenido" y destilda la casilla para Habilitar Java.



- Si eres la única persona en tu país usando Tor, se vuelve bastante obvio –el mismo usuario es el único que accede a las direcciones IP asociadas con nodos Tor. Si vas a usar Tor y estás preocupado de que un ISP pueda estar investigando el uso de Tor, podrías querer motivar a otros amigos a usar Tor – esto crea lo que los criptógrafos llaman "tráfico de cobertura". Quizás también quieras usar Tor para

leer varios sitios web, no sólo para publicar en tu blog. En ambos casos, esto significa que Tor está siendo usado para otras razones más que solo para publicar en tu blog anónimo, lo que significa que un usuario accediendo a Tor en los registros del servidor de un ISP no hará automáticamente que el ISP piense que algo malo está teniendo lugar.

Un pensamiento final sobre el anonimato: Si realmente no necesitas ser anónimo, no lo seas. Si tu nombre está asociado con tus palabras, las personas son más propensas a tomar tus palabras en serio. Pero algunas personas van a necesitar ser anónimas, y es por eso que esta guía existe. Sólo, por favor, no uses estas técnicas a menos que realmente lo necesites.