Scrivere un blog anonimo con Wordpress e Tor

La libertà di espressione passa anche dalla possibilità di comunicare proteggendo la propria identità, se necessario. Pubblico perciò qui una guida tecnica scritta da Ethan Zuckerman per *Global Voices*, di cui ho presentato le tecniche durante il convegno *e-privacy 2009* a Firenze. Di **Ethan Zuckerman** - originale - traduzione italiana di Jan Reister.

Introduzione

Una delle soddisfazioni di lavorare per Global Voices è stata la possibilità di collaborare con persone che esprimono le loro opinioni nonostante le forze che cercano di metterle a tacere. Ho lavorato con autori che volevano scrivere in rete su argomenti politici o personali, ma che per farlo dovevano essere certi che i loro scritti non potessero essere collegati alla loro identità. Questi autori sono attivisti dei diritti umani in decine di paesi, personale umanitario in paesi dal regime autoritario e whistleblower in aziende e governi.

Ho scritto una guida tecnica al blogging anonimo pubblicata su Global Voices qualche mese fa, in cui descrivevo alcuni metodi per tenere un blog in modo anonimo. Da allora ho tenuto workshop in tante parti del mondo ed ho apprezzato un particolare insieme di strumenti - Tor, Wordpress e vari account gratuiti di posta elettronica - che usati insieme possono offrire un alto livello di anonimato. Questa guida non esamina diverse direzioni di lavoro, ma ne propone una nel dettaglio spiegandola passo passo.

Puoi saltare le sezioni "perché" della guida, se hai fretta o se non ti interessa conoscere sempre i motivi di ogni cosa. In futuro spero di poter impaginare meglio le sezioni "perché" in modo da poterle comprimere ed espandere a piacere, abbreviando così l'intero documento.

Se nel documento sono stato poco chiaro od ho commesso errori, lasciamelo detto nei commenti - questa è una bozza che spero di perfezionare. Se pensi che sia utile e vuoi redistribuirla, fallo pure: è soggetta a una Creative Commons 2.5 Attribution license, che significa che puoi pure stamparla su delle tazzine da caffé e venderle, se pensi che ci sia un mercato per guadagnarci qualcosa. *[NdT: la traduzione è soggetta a licenza Creative Commons BY-NC-SA]*

Avvertenza

Se segui esattamente queste istruzioni ridurrai notevolemente la possibilità che si riesca a collegare la tua identità con i tuoi scritti in rete con metodi tecnologici-ad esempio, quando un organo dello stato o la polizia ottengono i dati da un Internet Service Provider. Purtroppo non posso garantire che questi metodi funzionino in ogni circostanza, né accetto alcuna responsabilità, civile o penale, qualora l'uso o l'abuso di queste istruzioni ti causasse problemi legali, civili o personali.

Queste indicazioni non impediscono che tu possa essere individuato tramite altri metodi tecnici, come il keystroke logging (l'installazione sul tuo computer di un programma che registra ogni tasto che batti) o la sorveglianza tradizionale (leggere lo schermo del tuo computer con una telecamera o un teleobiettivo). In realtà, la maggior parte delle persone viene identificata con mezzi non tecnologici a partire da ciò che scrive: talvolta scrive qualche indizio sulla sua vera identità, o si confida con qualcuno che si rivela inaffidabile. Non posso aiutarti su questo fronte, se non esortandoti a fare attenzione ed ad usare l'intelligenza. Per una guida migliore alle cose necessarie per essere "attenti e intelligenti" consiglio "How to blog safely" di EFF.

Ed ora le spiegazioni tecniche:

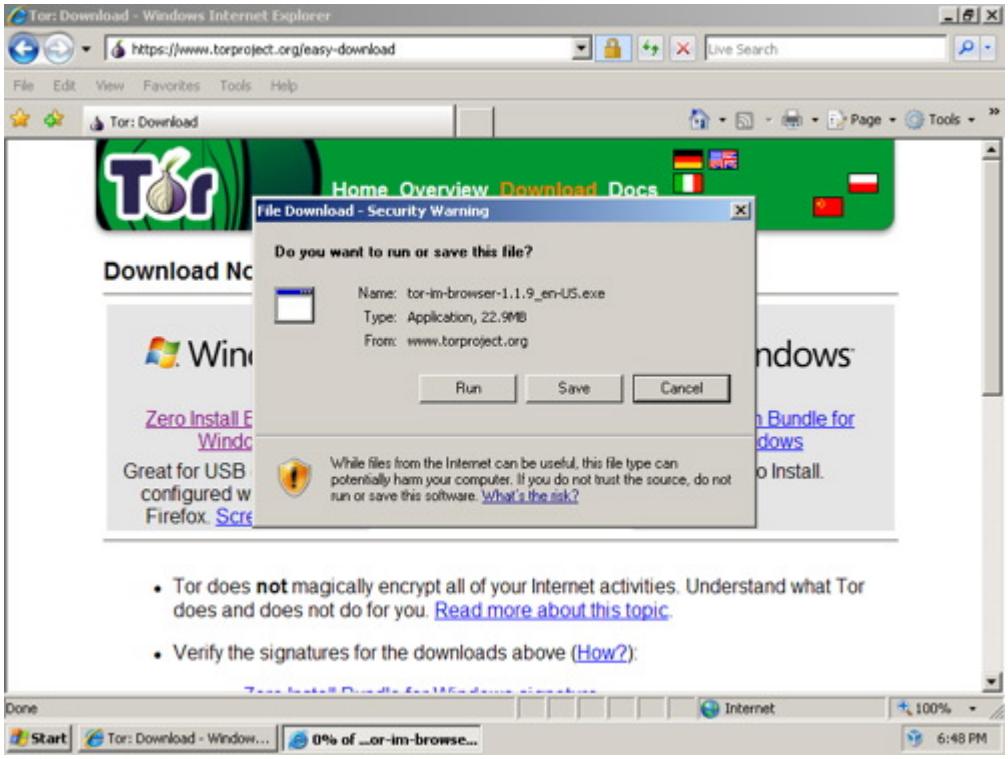
I - Scrivere da computer condivisi con altri

Se scriverai principalmente da computer condivisi (come i pc negli internet café) o se non puoi installare software su di un computer, segui le indicazioni qui sotto per usare Tor Browser Bundle senza dover installare permanentemente alcun software. Se invece scriverai prevalentemente dal tuo computer personale, dove puoi installare software, vai per favore al capitolo II.

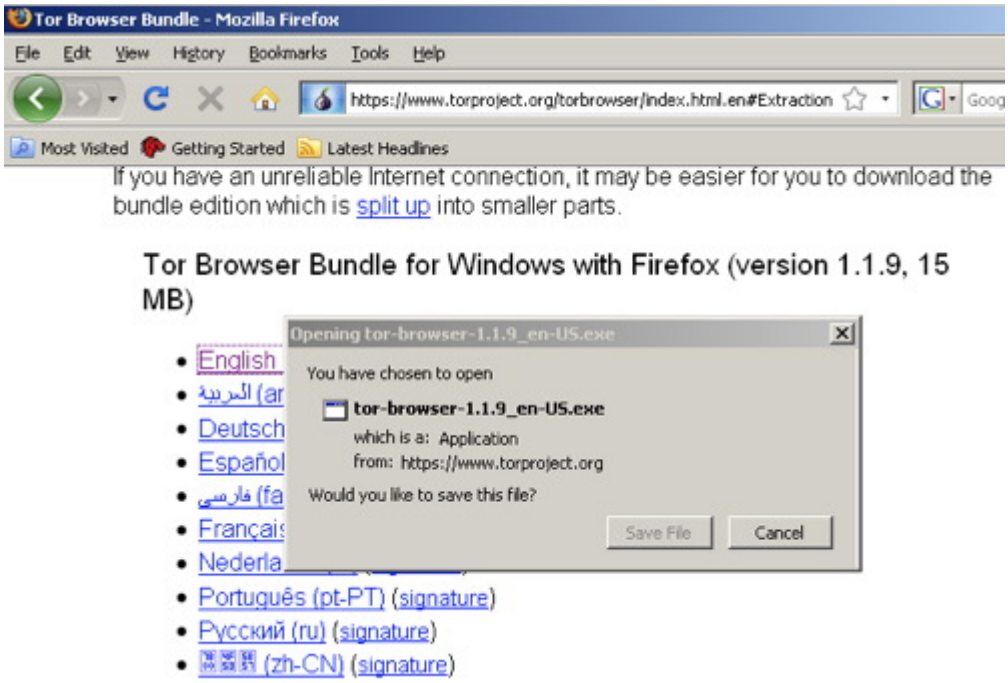
Tor Browser Bundle per Windows (per tutti i dispositivi portatili e penne USB)

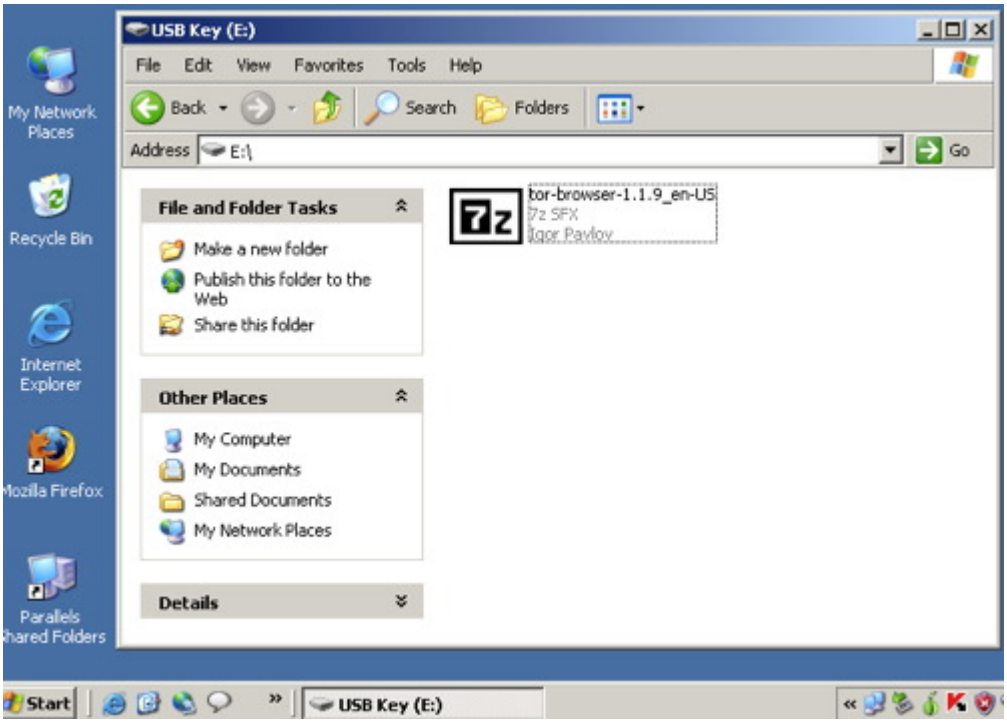
Consigliamo di scaricare Tor Browser Bundle per Windows, un ottimo pacchetto Tor preconfigurato con un browser Mozilla Firefox a sé stante per penne USB o per qualsiasi dispositivo portatile (schede SD, hard disk, schede compact flash). Tor Browser è una versione open source di un browser portatile, sviluppato dal Progetto Tor. E' una versione molto personalizzata per il browser Firefox con Tor, Vidalia, il caching proxy Polipo, Firefox e Torbutton già installati. E' progettato per essere messo su una chiavetta USB ed usare Tor da computer condivisi dove non è consentito installare software.

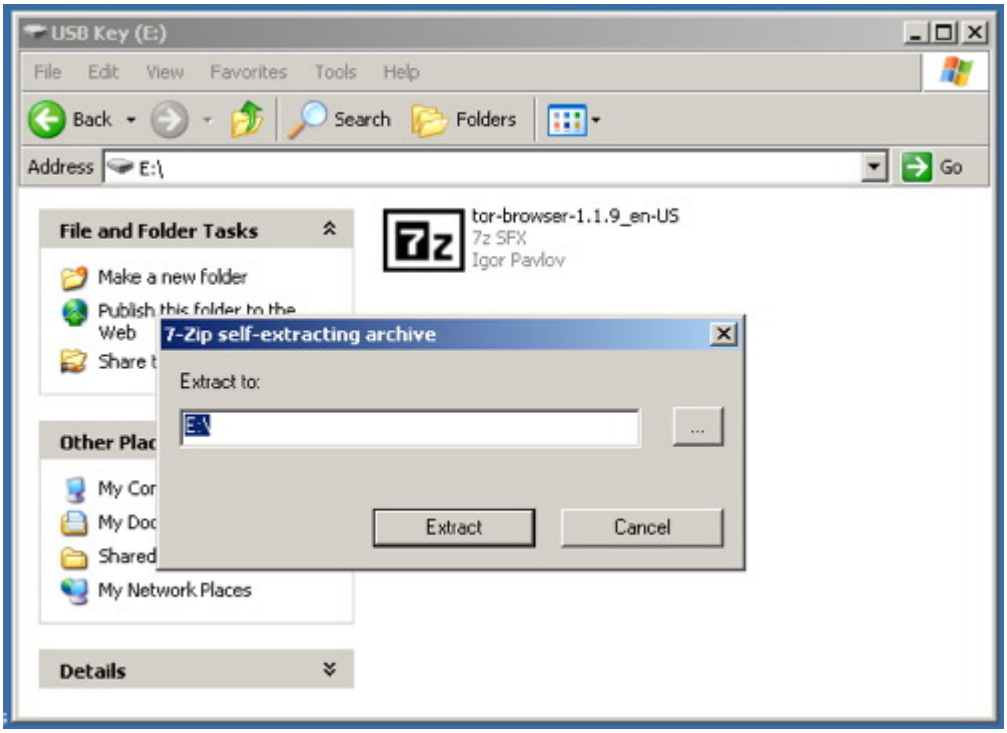
a) **Scarica il Tor Browser Bundle.** Dal sito web del Progetto Tor scarica il pacchetto nella tua lingua su di un computer dove poter salvare il file. Inserisci la tua penna USB e copia il Tor Browser Bundle. Con questa penna USB e qualsiasi computer dove sia possibile inserirla, potrai usare un browser protetto da Tor. Sul computer condiviso, chiudi il browser attivo. Inserisci la penna USB, trovane i file sul Desktop e fai doppio clic su Start Tor Browser.exe. Apparirà in breve tempo la finestra di Vidalia.

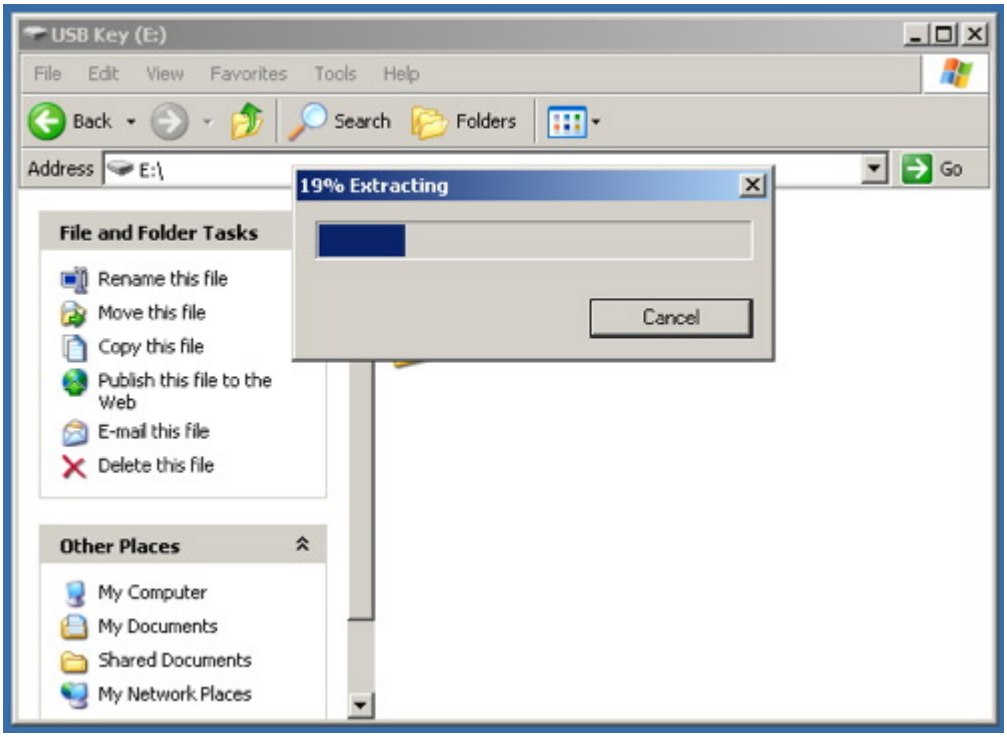


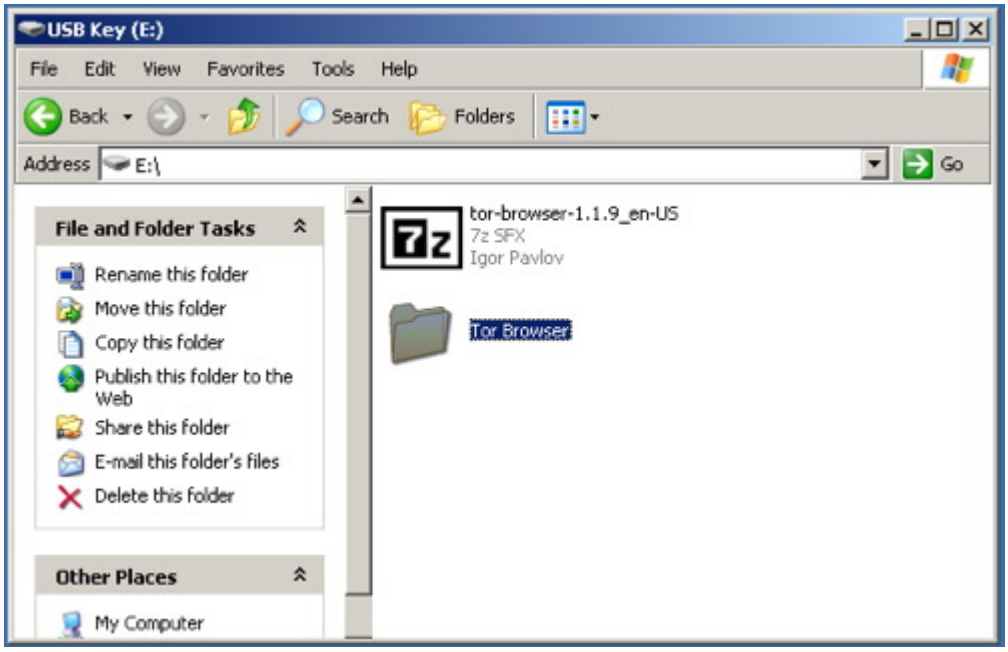
Ricorda che puoi scaricare il Tor Browser Bundle dal sito web del progetto Tor o scegliere il pacchetto nella tua lingua preferita dalla pagina di download del Tor Browser Bundle.

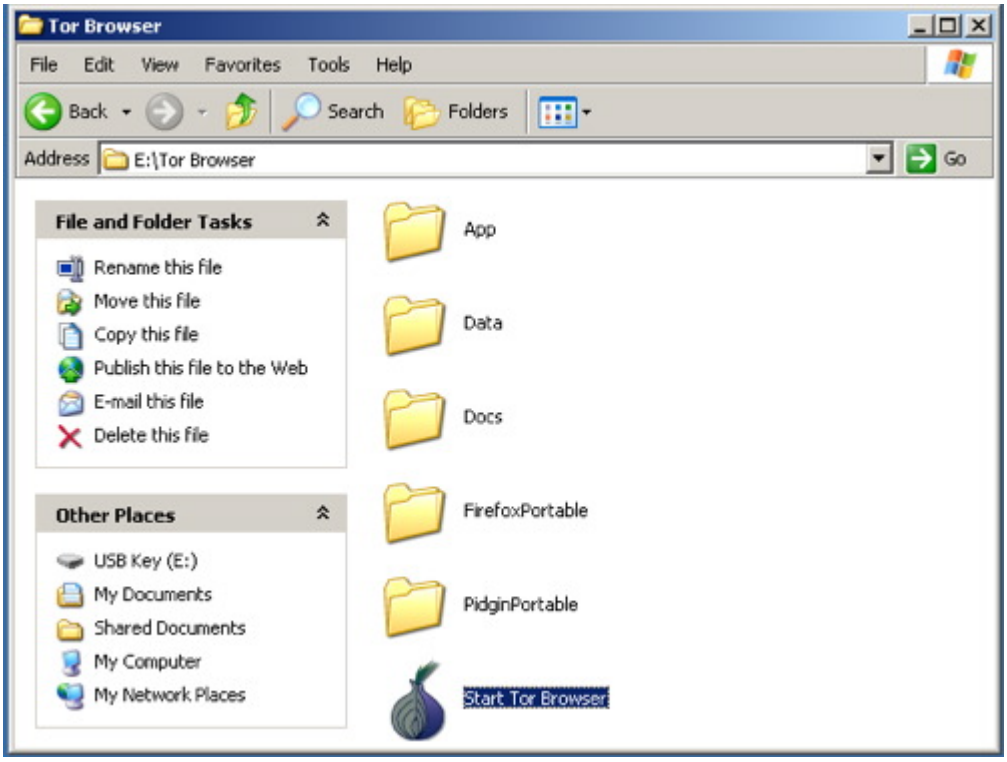


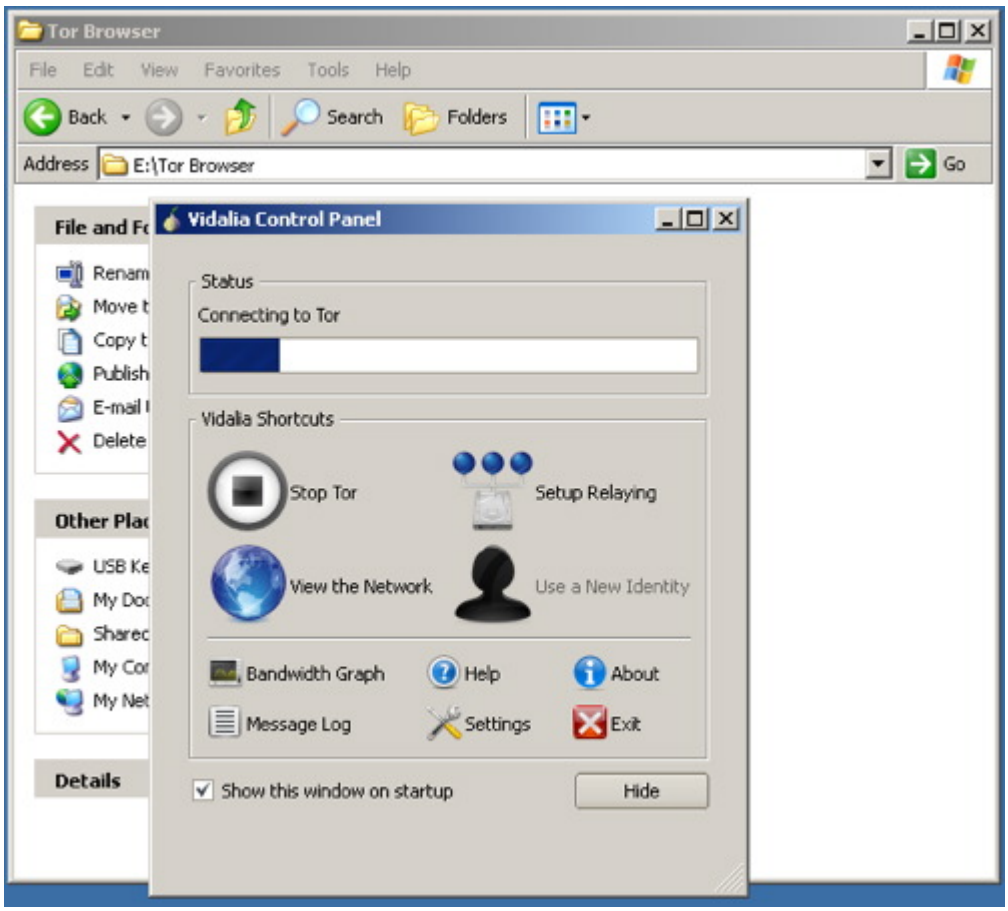

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
My Computer
My Documents
Shared Documents
My Network Places
Details
tor-browser-1.1.9_en-US
7z SFX
Igor Pavlov
My Network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

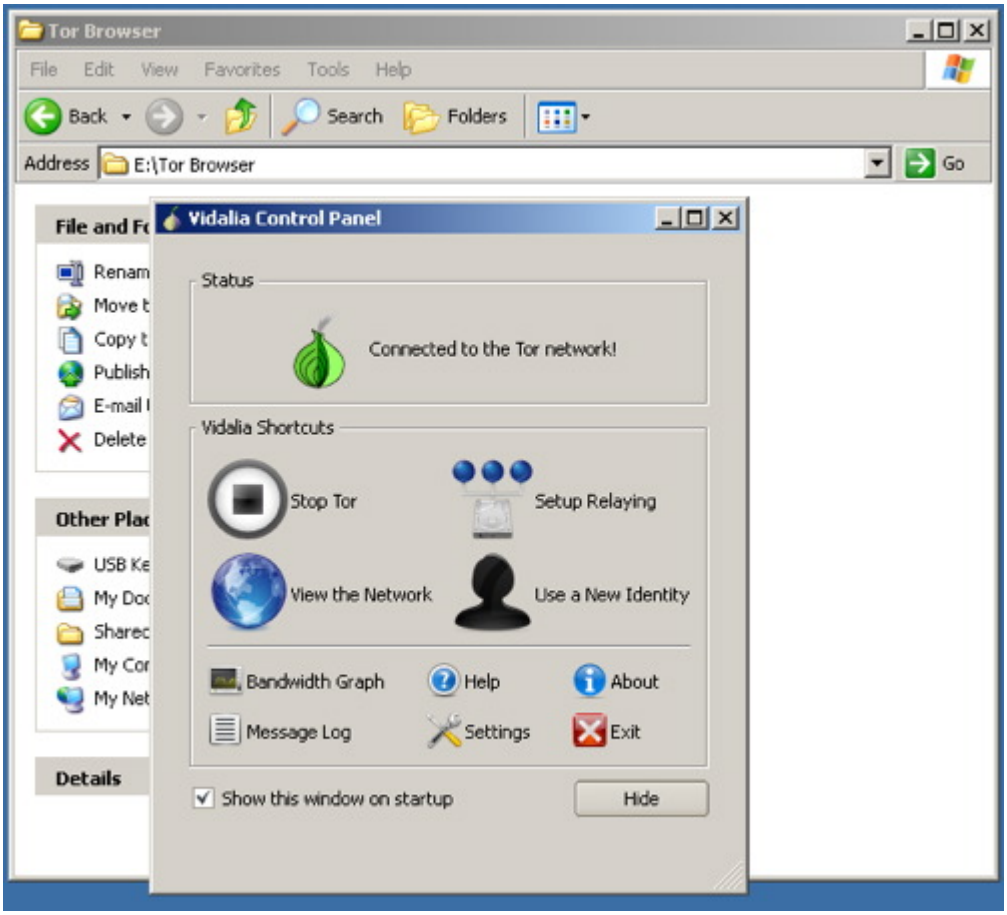

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
File and Folder Tasks
Make a new folder
tor-browser-1.1.9_en-US
7z SFX
Igor Pavlov
7-Zip self-extracting archive
Extract to:
E:\
...
Extract
Cancel
My Network Places
Details

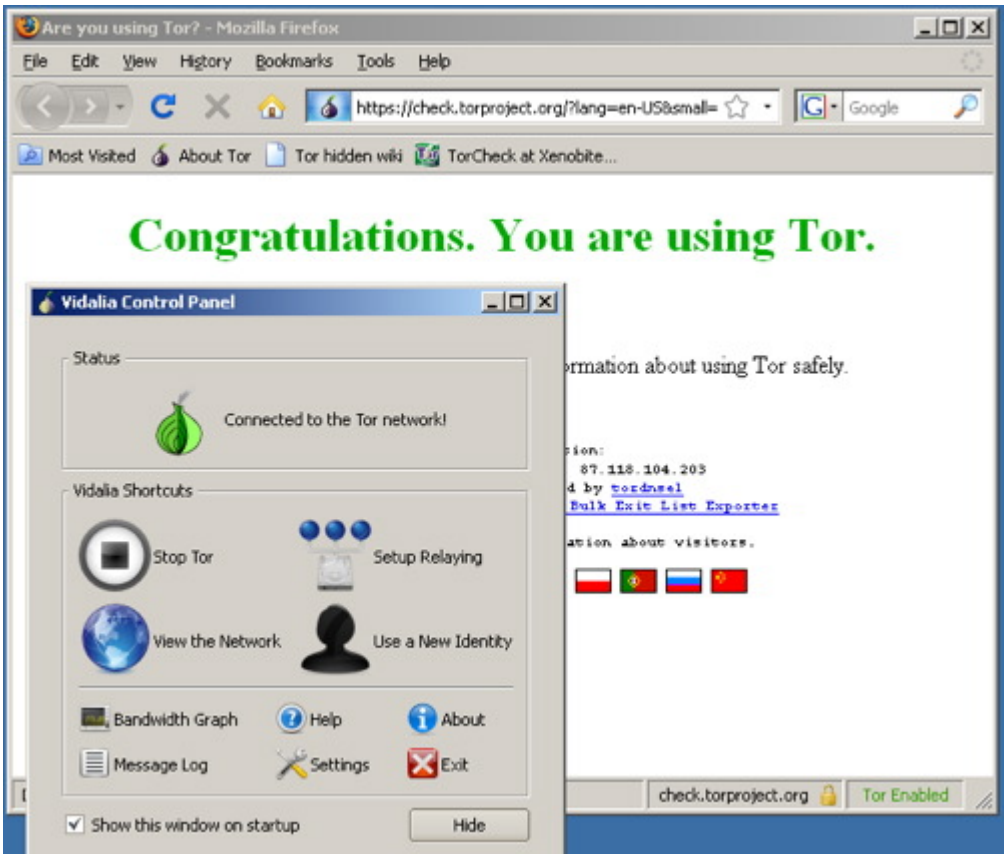

USB Key (E:)
File Edit View Favorites Tools Help
Back Search Folders
Address E:\
Go
19% Extracting
Cancel
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
My Computer
My Documents
Shared Documents
My Network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


Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.org/?lang=en-US&small=
Google
Most Visited
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Congratulations. You are using Tor.
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
check.torproject.org
Tor Enabled

b) **Estrai il file nella tua penna USB,** apri la cartella "Tor Browser" e fai clic su "Start Tor Browser". Dopo essersi collegato alla rete Tor, il browser Firefox con supporto Tor partirà automaticamente e visiterà la Tor Test Page. Controlla che ci sia il messaggio "Congratulazioni. Stai usando Tor.". Altrimenti otterrai il messaggio "Spiacente. Non stai usando Tor. Se stai cercando di usare un client Tor, leggi il sito web di Tor ed in particolare le istruzioni per configurare il client Tor."

II - Scrivere dal proprio computer personale

Se scriverai principalmente dal tuo computer personale, su cui puoi installare software, segui queste istruzioni.

1: maschera il tuo indirizzo IP

Ogni computer in Internet ha o condivide un indirizzo IP. Questi indirizzi non sono degli indirizzi fisici, ma possono permettere ad un bravo amministratore di sistema di rintracciare il tuo indirizzo reale. In particolare, se lavori per un ISP puoi facilmente associare un indirizzo IP al numero di telefono che ha usato quell'IP in un certo momento. Così, prima di qualsiasi operazione anonima in Internet, bisogna mascherare il nostro IP. Cosa fare se vuoi tenere un blog dal computer di casa o del lavoro:

a) **Installa Firefox.** Scaricalo dal sito di Mozilla ed installalo sul computer principale che usi.

Perché?

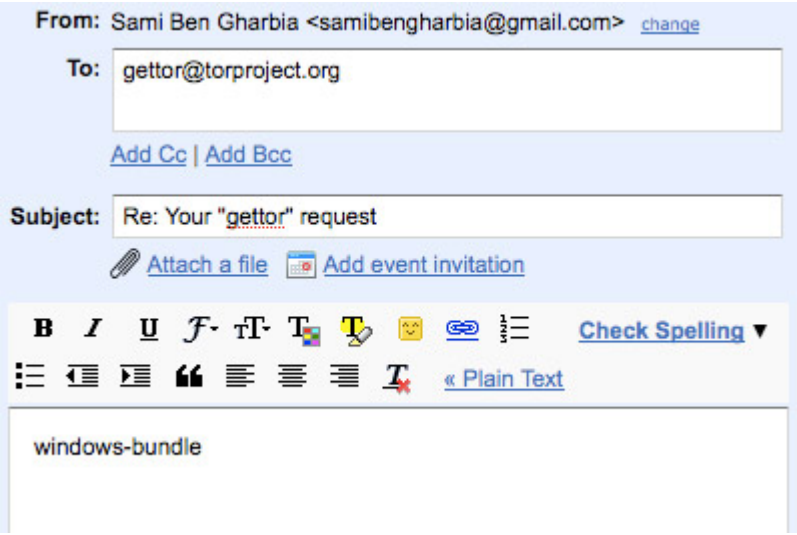
Internet Explorer ha dei discreti problemi di sicurezza che possono compromettere la tua sicurezza in rete. Questi problemi tendono a restare irrisolti molto più a lungo in IE che in altri browser. (Non ci credi? Chiedilo a Bruce Schneier) E' il browser più vulnerabile allo spyware che si scarica inavvertitamente da siti web. Inoltre, molti degli strumenti per la privacy sviluppati ora sono stati scritti specificamente per funzionare con Firefox, come Torbutton, che useremo nei passi successivi.

b) **Installa Tor.** Scarica il programma dal sito web Tor. Se nel tuo paese l'accesso al sito web principale di Tor è bloccato, ci sono alcuni mirror in altri posti da cui scaricarlo. Puoi anche consultare la cache di Google per leggervi la pagina dei mirror cercando "site:torproject.org mirrors". Scegli l'ultima versione stabile per la tua piattaforma e scaricala sul tuo desktop. Segui le istruzioni indicate con un link a destra accanto alla versione scaricata. Installerai due pacchetti software e dovrai effettuare alcune modifiche alla tua installazione di Firefox.

Nel caso che la tua connessione a internet blocchi l'accesso al sito web Tor, puoi richiedere un pacchetto spedendo una email al robot "gettor" all'indirizzo gettor (AT) torproject (DOT)

org. Nota bene: le email per gettor @ torproject . org devono provenire da un account Gmail, altrimenti non avranno risposta. Scegli uno dei seguenti nomi di pacchetti e scrivilo nel corpo dell'email:

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



Poco dopo l'invio dell'email, riceverai una risposta dal robot "gettor" col software richiesto in un file zip. Apri il file zip e 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.

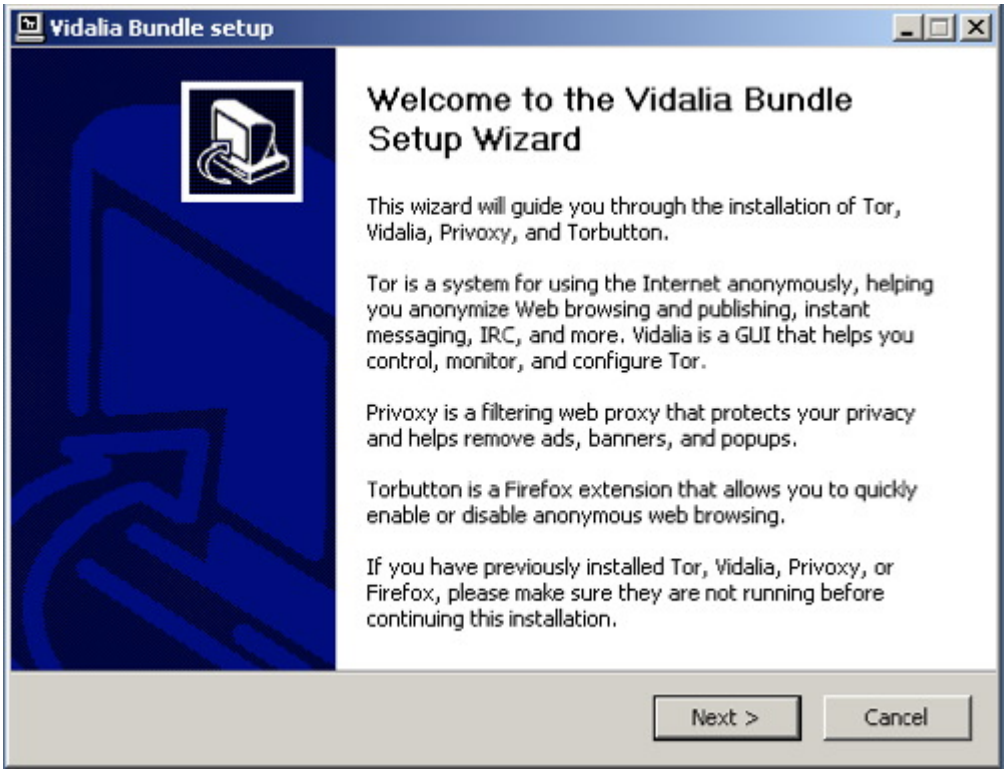
You can acquire a bridge by sending an email that contains "get bridges" in the body of the email to the following email address: bridges@torproject.org

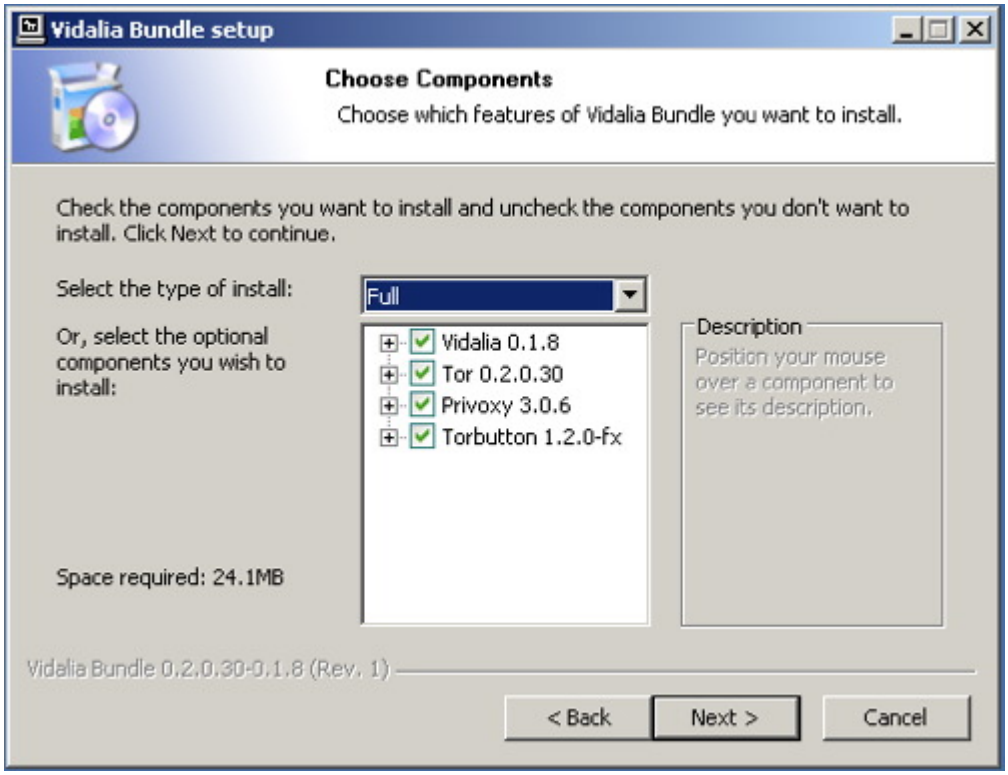
It is also possible to fetch bridges with a web browser at the following url: https://bridges.torproject.org/

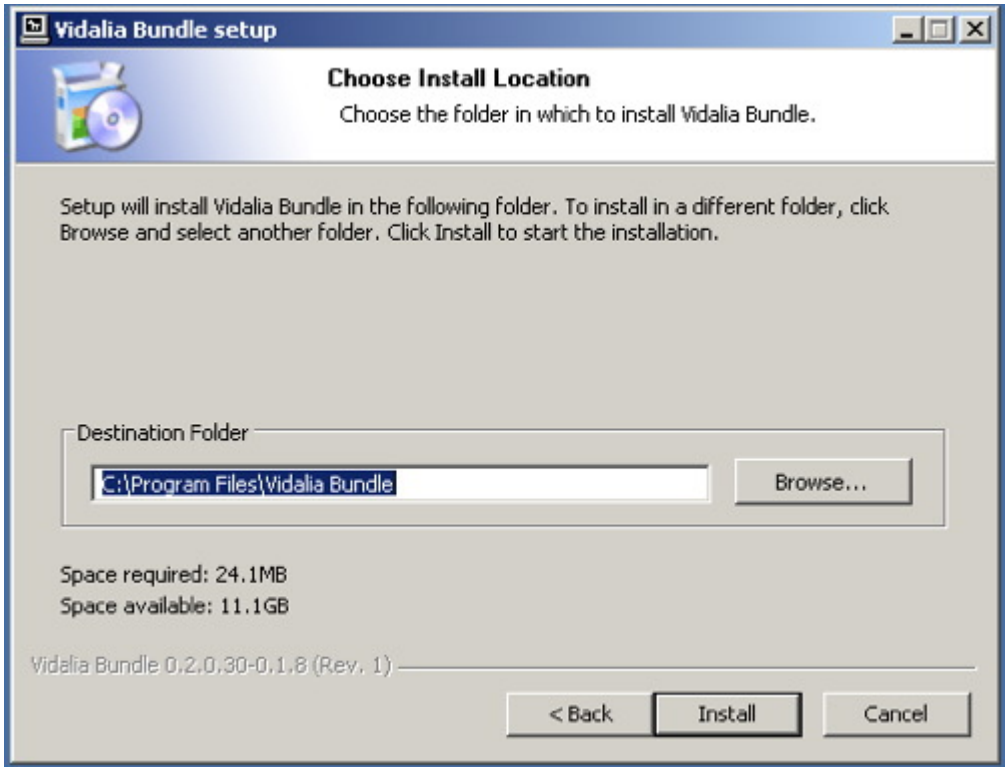
- Show quoted text -

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

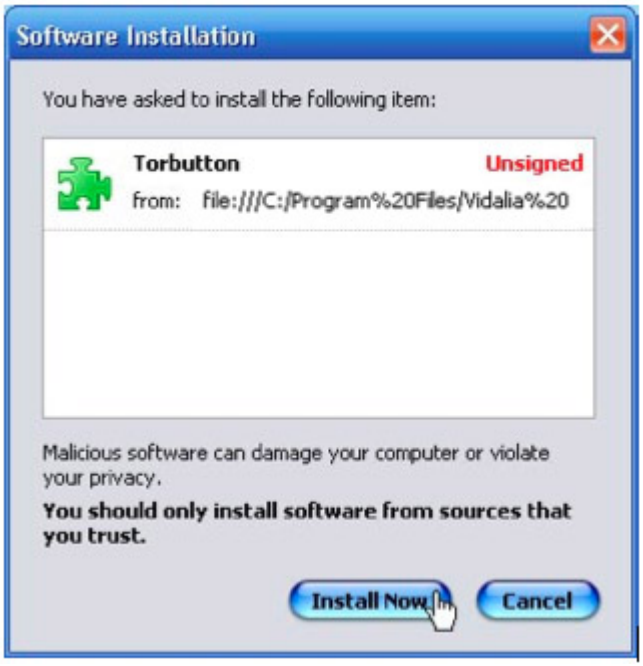

Vidalia Bundle setup
Choose Components
Choose which features of Vidalia Bundle you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Full
Or, select the optional components you wish to install:
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



Perché?

Tor è una rete molto sofisticata di proxy server. Essi richiedono le pagine web al tuo posto, in modo che il server web di destinazione non veda l'indirizzo IP originale del computer che ha richiesto la pagina. Usando Tor, usi a cascata tre particolari proxy server per recuperare ciascuna pagina web. Le pagine vengono cifrate nel passaggio tra i server Tor, ed anche quando uno o due dei server nel circuito fossero compromessi, sarebbe molto difficile capire quale pagina web stavi leggendo o su quale pagina stavi scrivendo. Tor installa anche un altro software, Privoxy, che aumenta la sicurezza del tuo browser bloccando cookie ed altro software che consentirebbe il tracciamento. Blocca inoltre molta della pubblicità che si trova sul web.

c) **Il pacchetto installa anche il plugin Firefox Torbutton**. Chiederà semplicemente di potersi installare. Fai clic su "Installa Ora", riavvia Firefox ed è pronto:



Perché?

Impostare manualmente Tor significherebbe doversi ricordare di cambiare le preferenze del browser ed usare un proxy server. E' un processo lungo che spesso ci si dimentica di completare. Con Torbutton basta un clic del mouse ed è anche facile sapere se si sta usando o meno Tor, cosa molto utile.

Troverai che Tor rallenta l'uso del web - dipende dalle richieste Tor che vengono istradate attraverso tre proxy prima di raggiungere il web server di destinazione. Alcuni - me compreso - usano Tor solo quando è importante nascondere la propria identità, e lo spengono se non serve - con Torbutton è molto facile.

d) **Attiva Tor in Firefox e provalo.** Con Tor attivo, visita questo indirizzo). Se ottieni questo messaggio: "Congratulazioni. Stai usando Tor.", allora tutto è stato installato correttamente e sei pronto per il prossimo passo.

Altrimenti otterrai il messaggio "Spiacente. Non stai usando Tor. Se stai cercando di usare un client Tor, leggi il sito web di Tor ed in particolare le istruzioni per configurare il client Tor."

Perché?

E' sempre bene verificare che il software installato funzioni, specie quando è così importante come Tor. La pagina che visiti controlla da quale indirizzo IP proviene la tua richiesta. Se proviene da un nodo Tor conosciuto, Tor funziona correttamente ed il tuo IP è nascosto - altrimenti, c'è qualcosa che non va e dovresti capire perché Tor non funziona correttamente.

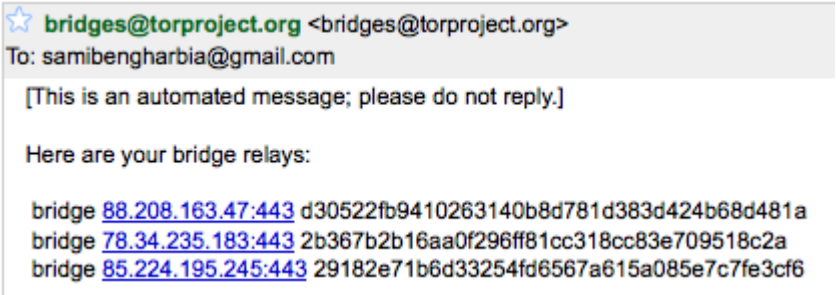
Cosa fare se Tor non si connette mai?

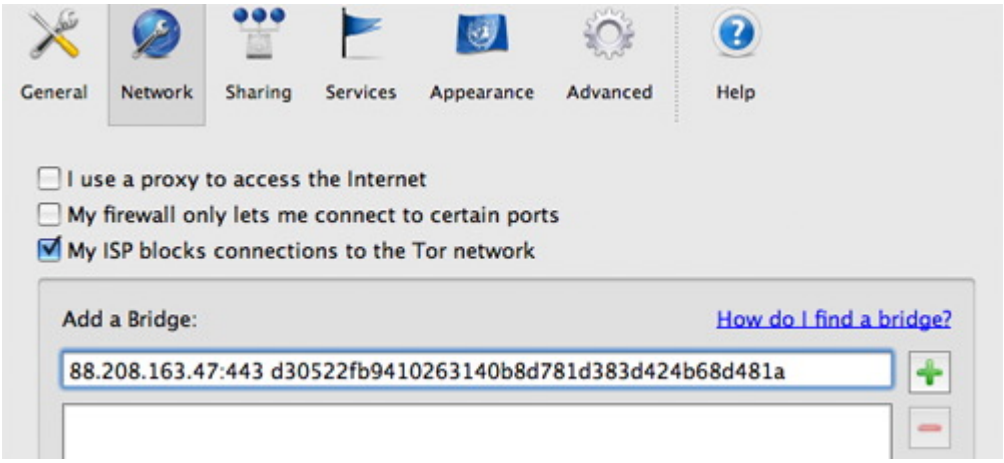
Se hai difficoltà a collegarti alla rete Tor, leggi la FAQ sui problemi di funzionamento di Tor Nel caso in cui la tua connessione ad Internet blocchi l'accesso alla rete Tor, e nel caso che l'icona di Vidalia sia sempre gialla, puoi considerare l'uso dei bridgerelay. E' il secondo passo logico per collegarsi alla rete Tor.

I bridge relay (https://www.torproject.org/bridges) (o "bridges") sono relay Tor non elencati nella directory principale Tor. Non essendocene una lista completa, anche se il tuo ISP filtrasse le connessioni verso tutti i relay Tor conosciuti, probabilmente non riuscirebbe a bloccare tutti i bridge. Se sospetti che ti venga bloccato l'accesso alla rete Tor, puoi provare ad usare i bridge.

Puoi avere un bridge spedendo una email, da un account gmail, contenete "get bridges" nel corpo del messaggio, all'indirizzo bridges @ torproject . org . In breve riceverai una risposta automatica contenente i bridge. Si possono ottenere dei bridge anche da qui: https://bridges.torproject.org/

Apri il pannello di controllo di Vidalia, vai a Impostazioni > Rete e fai clic su "Il mio ISP blocca le connessioni alla rete Tor". Aggiungi uno alla volta l'indirizzo di ciascun bridge incollandolo nella finestra "Aggiungi un bridge" e facendo clic sul segno "+".





2: Crea un indirizzo email nuovo e difficile da rintracciare.

Molti servizi web, compresi quelli che ospitano blog, richiedono un indirizzo email per poter comunicare con i loro utenti. Per i nostri scopi questo indirizzo email non può essere collegato a informazioni personali e identificanti, come l'indirizzo IP che usiamo per iscriverci al servizio. Perciò ci serve un nuovo account email da creare usando Tor, facendo attenzione che nessun dato usato - nome, indirizzo etc. - sia collegabile a noi. NON devi usare un indirizzo email esistente - è probabile che ti ci sia iscritto da un indirizzo IP non nascosto, ed in genere i fornitori di webmail conservano l'indirizzo IP usato per la creazione.

a) **Scegli un fornitore di webmail** - Consigliamo Riseup.net e Gmail, ma fintanto che usi sempre Tor potresti anche usare anche Yahoo o Hotmail. Puoi anche registrarti un account webmail gratuito e rapido con fastmail.fm.

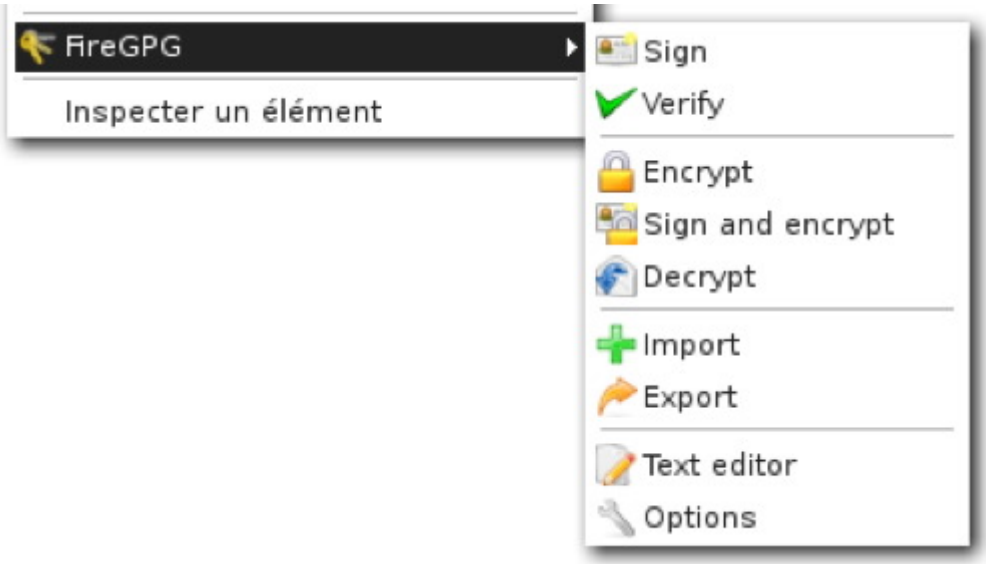
Perché?

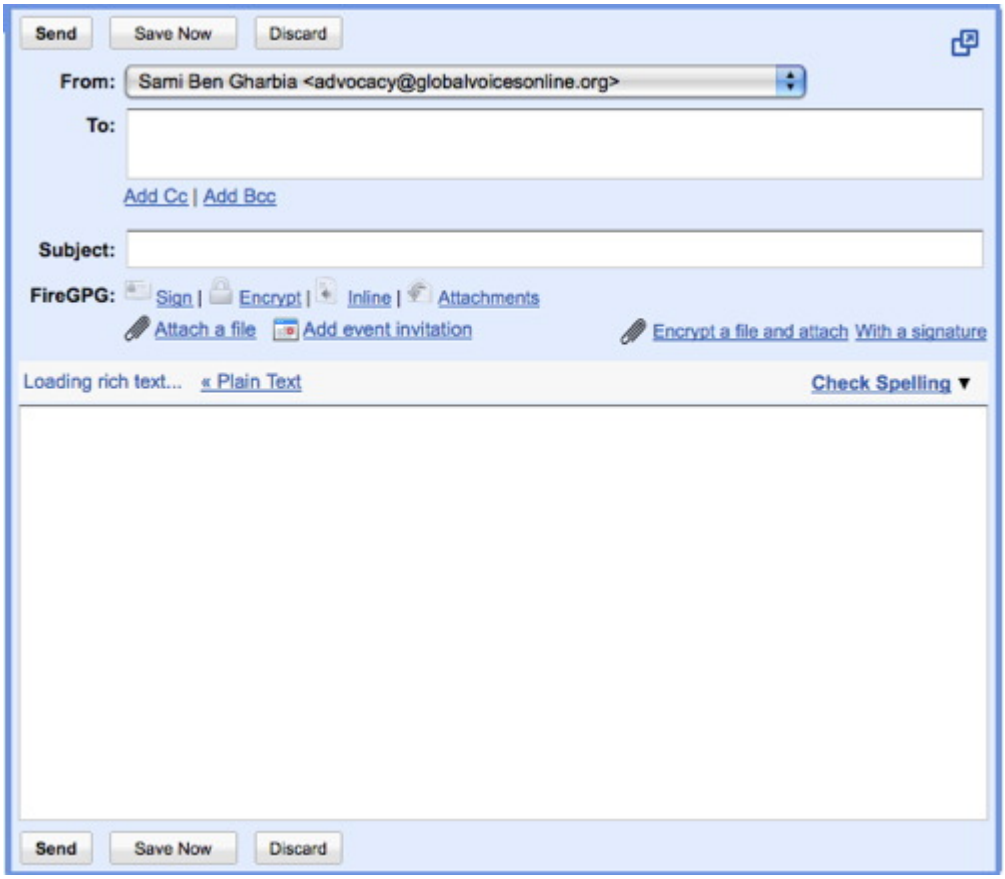
La webmail è il modo migliore per creare un indirizzo email "usa e getta" che puoi usare per iscriverti ai servizi e poi ignorare. Molti utenti però usano la webmail anche come loro email principale. Se anche tu lo fai, è importante capire i punti di forza e di debolezza dei diversi fornitori di posta.

Hotmail e Yahoo hanno entrambi una "funzione di sicurezza" che disturba parecchio chi ama la privacy. Includono entrambi l'indirizzo IP del computer usato per inviare la posta. Ciò è comunque irrilevante se accedi a questi servizi via Tor, dato che l'indirizzo IP sarà un indirizzo IP Tor e non il tuo indirizzo. Inoltre Hotmail e Yahoo non offrono accesso sicuto (https) alla webmail - ancora, questo conta poco finché usi Tor ogni volta che usi questi servizi email. Ma molti utenti vogliono controllare la posta in circostanze in cui non hanno Tor a disposizione - per il tuo account email principale vale la pena scegliere un fornitore che abbia accesso https alla webmail.

Riseup.net offre una webmail con elevata sicurezza. Supportano la cifratura con PGP (Pretty Good Privacy) - molto utile se sei in corrispondenza con persone che usano PGP anch'esse. Puoi richiedere un account gratuito su www.riseup.net e chiedere ai tuoi corrispondenti di fare altrettanto.

Gmail ha alcune funzionalità di sicurezza interessanti anche se non si propone come un servizio di email sicuro. Se visiti questo indirizzo speciale https://mail.google.com/mail tutta la sessione con Gmail viene cifrata con https. Puoi anche visitare https://mail.google.com/mail/h/ che è una webmail Gmail sicura con interfaccia Basic HTML. (Io consiglio di segnare questo indirizzo nei segnalibri ed usarlo per tutte le sessioni Gmail.) Gmail non inserisce l'indirizzo IP nell'intestazione dell'email e puoi avere supporto PGP usando FireGPG, un'estensione Firefox che aggiunge crittografia forte a Gmail. FireGPG ha un'interfaccia per decifrare, cifrare, firmare e verificare la firma al testo di qualsiasi pagina web tramite GnuPG.





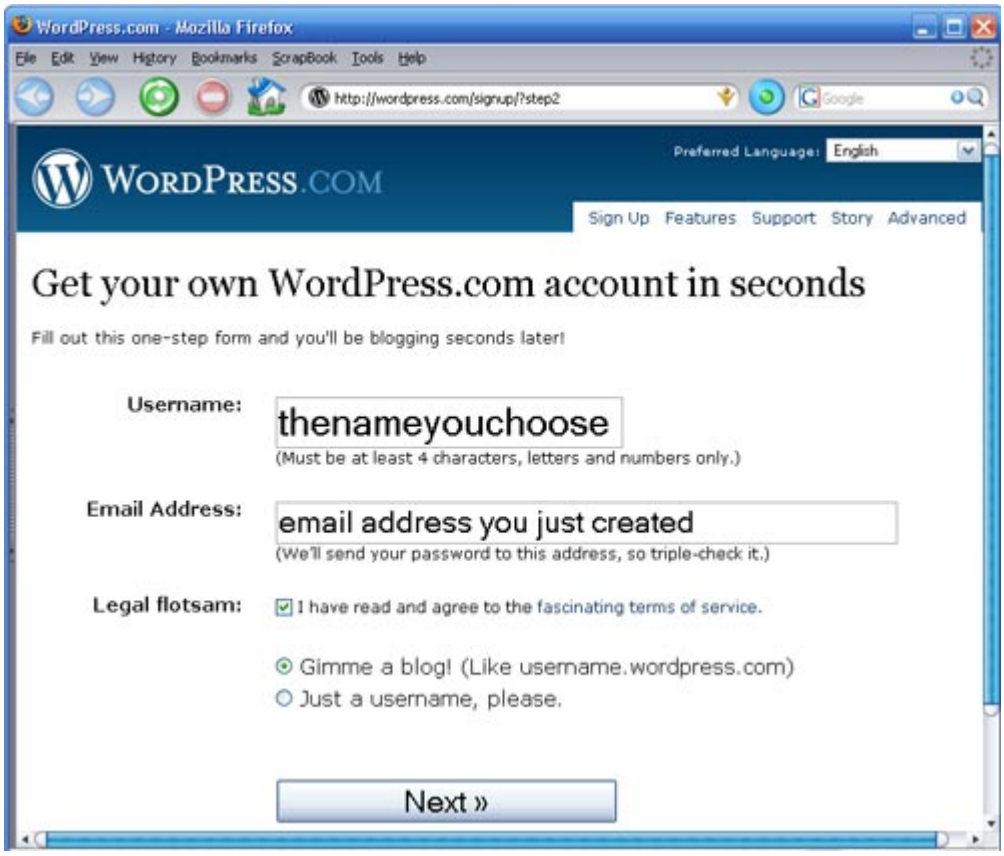
Un'avvertenza a tutti gli utilizzatori di account webmail - stai affidando tutta la tua posta all'azienda che gestisce il servizio. Se l'azienda viene compromessa da hacker, o se viene costretta dal governo a rivelare informazioni, altri avranno accesso al testo di tutte le email che hai ricevuto e spedito. L'unica alternativa è scrivere le tue email in un editor di testo, cifrarle sul tuo computer con PGP ed inviarle a qualcuno che usi PGP pure lui. Questo livello di sicurezza è al di là di ciò che la maggioranza di noi desidera e richiede, ma è importante ricordare che ti stai fidando di un'azienda che potrebbe non avere a cuore i tuoi stessi interessi. Yahoo in particolare ha la pessima abitudine di passare informazioni al governo cinese - alcuni dissidenti cinesi stanno facendo causa all'azienda per la comunicazione illegale dei loro dati. E' qualcosa a cui pensare quando si deve scegliere di chi fidarsi...

b) **Avvia Tor nel tuo browser**, o avvia Tor Browser dalla tua penna USB. Visita il sito di email di tua scelta e iscriviti per un nuovo account. Non usare informazioni personali che ti possano identificare - pensa di diventare una persona dal nome banale in un paese con molti utenti web, come gli USA o il Regno Unito. Scegli una password robusta (almeno dodici caratteri, con almeno un numero e un carattere speciale) per l'account e scegli un nome utente simile al nome che userai per il tuo blog.

c) **Controlla di riuscire fare login al servizio email** ed invia una email di prova (non ad un indirizzo tuo o di conoscenti) con Tor attivo. Di solito Tor cambia circuito ogni 10 minuti e ciò potrebbe disturbare le operazioni della webmail, così puoi dedicare massimo 10 minuti a scrivere ogni email.

3: registra il tuo nuovo blog anonimo

a) **Avvia Tor nel tuo browser**, o avvia Tor Browser dalla tua penna USB. *Visita Wordpress.com ed iscriviti per un nuovo account* facendo clic sul link "Sign Up Now!". Usa l'indirizzo email appena creato e crea un nome utente che sarà parte dell'indirizzo del tuo blog: ilnomechescegli.wordpress.com



b) Wordpress invierà un link di attivazione al tuo account webmail. Usa il browser con Tor per leggere quella email e **fare clic sul link di attivazione.** Così Wordpress sa che hai usato un indirizzo email attivo e che può comunicarti aggiornamenti del servizio - il risultato è che renderanno pubblico il tuo blog e ti invieranno la tua password. Devi controllare ancora la webmail per recuperare la password.

c) Sempre usando Tor, fai login nel tuo nuovo blog usando username e password. Fai clic su "Il Mio Account" e su "Modifica Profilo". **Cambia la tua password** con una password forte che riesci a ricordare bene. Aggiungi pure delle informazioni al tuo profilo... basta che non siano collegabili a te!

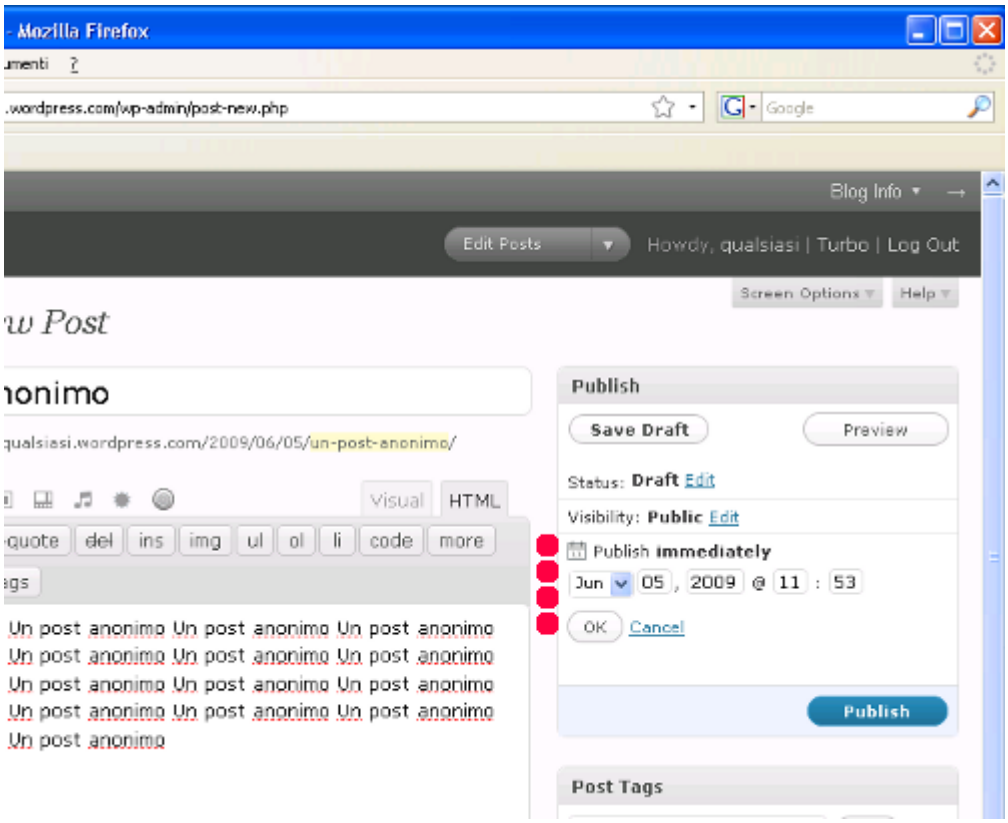
4: Scrivi sul tuo blog

a) **Scrivi il tuo articolo offline.** E' un buon metodo per non perdere un post se il browser si blocca o il collegamento a Internet cade, ma serve anche a scrivere i propri articoli in un

luogo più privato di un internet café. Un semplice editor come Blocco Note per Windows è spesso la scelta migliore. Salva i tuoi articoli come file di testo (dopo avere scritto sul blog ricordati di cancellarli completamente dal tuo computer con strumenti quali Eraser o Ccleaner che sono disponibili in molte lingue e cancellano i file temporanei automaticamente da tutti i browser installati e da altre applicazioni).

b) Avvia Tor, o usa Tor Browser dalla tua penna USB e fai login su Wordpress.com. Fai clic su "Articoli > Add New" per scrivere un nuovo post. Copia e incolla l'articolo dal tuo file di testo alla finestra del post. Metti un titolo e scegli le categorie che vuoi.

c) Prima di fare clic su Pubblica c'è un passaggio cruciale. Fai clic sulla voce a destra che dice **"Pubblica subito o Modifica"**. Scegli una data di qualche minuto nel futuro - idealmente, scegli un intervallo casuale e usa un tempo diverso ogni volta. Questo ritarderà la pubblicazione del post sul tuo blog - Wordpress non renderà pubblico il post finché non arriverà il momento indicato.



Modificando l'ora di pubblicazione ci si protegge da una tecnica per determinare la tua identità. Immagina di scrivere su un blog detto. Modificando l'ora di pubblicazione questo attacco è più difficile per l'Internet Service Provider. Avrebbe bisogno anche dei log del server Wordpress, che sono molto più difficili da ottenere. Si tratta di una protezione molto facile che aumenta la propria sicurezza.

5: Copri le tue tracce

a) Cancella in modo sicuro le bozze dell'articolo fatte sul tuo laptop o computer di casa. Se ti serve una penna USB per portare l'articolo all'internet café, devi cancellare anche quella. Non basta mettere il file nel cestino e svuotarlo - devi usare uno strumento di cancellazione sicura come Eraser o Ccleaner che sovrascrivono il vecchio file con dati che lo rendono impossibile da recuperare. Sul Macintosh questa funzione è nativa - metti un file nel cestino e seleziona "Vuota il cestino in modalità sicura" dal menu del Finder.

b) Cancella la cronologia di navigazione, i cookie e le password da Firefox. Dal menu Strumenti, seleziona "Elimina i dati personali". Spunta tutte le opzioni e fai clic su "okay". Potresti configurare Firefox per cancellare automaticamente questi dati ogni volta che esci - puoi farlo in "Modifica > Preferenze > Privacy" e spunta la voce che dice "Elimina sempre i dati personali alla chiusura di Firefox". Se non puoi installare programmi sul computer, usa lo strumento IE Privacy Cleaner dalla penna USB per cancellare i dati temporanei del browser.

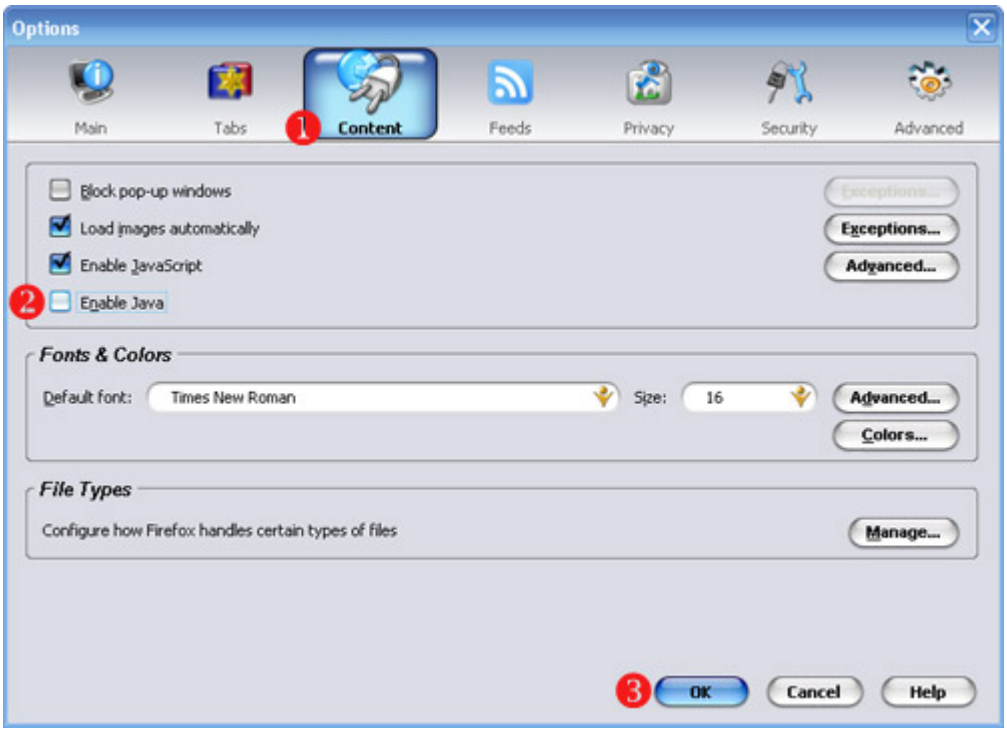
Perché? E' facile capire quali siti web hai visitato esaminando la cronologia del browser. Un esame più approfondito può rivelare la cronologia dai file di cache, che contengono le versioni delle pagine visitate. Questi dati vanno cancellati da un computer pubblico, in modo che il prossimo utente non li trovi. E vanno eliminati anche dal proprio computer, in modo che se venisse perso, rubato o sequestrato non sia possibile essere messi in relazione agli articoli che abbiamo scritto.

Alcune osservazioni conclusive:

- Non basta proteggersi mentre si scrive sul proprio blog. Se scrivi commenti su altri blog usando il nome del tuo blog anonimo, devi farlo usando Tor. Le piattaforme di blog registrano l'IP dei commenti - se non usi Tor, inviti chiunque gestisca quel sito a

rintracciare il tuo IP ed il tuo computer. Tor è come un preservativo: non fare blogging insicuro.

- Anche se sei anonimo, puoi sempre abbellire il tuo blog. La voce "Aspetto" in Wordpress ha molte opzioni da provare - template diversi, foto e personalizzazioni. Ma sii estremamente cauto se usi le tue foto - una foto contiene moltissime informazion su di te (se è stata fatta in Zambia, prova il fatto che eri in Zambia).
- Se sei veramente preoccupato della tua sicurezza, fai un altro passo per configurare il browser Firefox e disabilita Java. C'è un brutto difetto di sicurezza nella versione più recente di Java, che permette all'autore di uno script malizioso di capire qual'è l'indirizzo IP del tuo computer anche se stai usando Tor. Noi non ce ne curiamo troppo perché non pensiamo che Wordpress.com o Google usino questi script, ma è qualcosa da considerare seriamente se usi Tor per altre ragioni. Per disattivare Java, vai in "Modifica > Preferenze > Contenuti" e togli la spunta ad "Attiva Java" (Tor Browser Bundle disattiva Java di default).



- Se sei l'unica persona del tuo paese ad usare Tor, è ovvio che l'utente che accede agli indirizzi IP legati a Tor è sempre lo stesso. Se vuoi usare Tor e ti preoccupa che un ISP indaghi sull'uso di Tor, potresti incoraggiare degli amici ad usare Tor - ciò crea quello che i crittografi chiamano "traffico di copertura". Puoi anche usare Tor per visitare vari siti web, non solo scrivere sul tuo blog. In entrambi i casi significa che Tor viene usato per altre ragioni oltre a postare sul tuo blog anonimo, così se nei log di un ISP un utente accede a Tor ciò non indurrà automaticamente l'ISP a pensare che stia accadendo qualcosa di brutto.

Un'ultima considerazione sull'anonimato: Se non hai veramente bisogno di essere anonimo, non esserlo. Se il tuo nome è associato alle tue parole, è più facile che la gente prenda sul serio ciò che scrivi. Tuttavia, alcune persone hanno bisogno di restare anonime, ed

è per questo che esiste questa guida. Solo, per favore non usare queste tecniche se non ne hai davvero bisogno. fine. --