Istruzioni e consigli per l'uso di Tor Browser (aggiornamento del 23 agosto 2020)

Cari compagni e sinceri democratici,
queste istruzioni hanno lo scopo di permettervi di non essere individuati quando operate su Internet.
TOR permette di non essere individuati quando scambiate messaggi con altre persone: con la riserva che l'anonimato è garantito completamente solo se anche l'altra persona usa TOR. Prima di usare TOR dovete aver ben chiaro che siete anonimi in quanto chi vi spia non è in grado di sapere chi e da dove inviate un messaggio. Ma se il messaggio non è criptato il suo contenuto è leggibile dagli spioni. Quindi è necessario imparare anche l'uso del sistema di criptazione PGP: sul sito del (n)PCI al link: http://www.nuovopci.it/contatti/infocont.html trovate il manuale con istruzioni e consigli per l'uso del PGP.
Delle istruzioni che seguono, le cose importanti sono i consigli sull'uso di TOR. Una volta installato, il suo uso è semplice, ma solo seguendo i consigli qui dati evitate di rivelare la vostra identità.
Voler migliorare la società, cambiare lo stato delle cose è illegale per chi detiene il potere nelle cosiddette "democrazie occidentali". Quindi armatevi degli strumenti tecnici adatti a cambiare lo stato attuale delle cose.

Le istruzioni sono divise in capitoli. All'interno di ogni capitolo abbiamo numerato i paragrafi: questo perché ogni eventuale nostro corrispondente che ha osservazioni da fare su qualche istruzione, possa indicare facilmente a quale si riferisce.

INDICE

1. Procurarsi il programma per l'installazione di Tor Browser

1. All'indirizzo internet che segue trovate il programma per installare Tor Browser **(1)** per Windows e altri sistemi operativi: **https://www.torproject.org/download/**

> **(1) Tor Browser** è un programma che integra Firefox e TOR e non ha bisogno di nessun altro programma accessorio per funzionare, né di impostazioni da parte di chi lo utilizza.
> TOR funziona anche su altri sistemi operativi (Mac OS, Linux e Android).

2. **Nota bene** che le istruzioni che seguono per l'installazione sono riferite a Windows 10.

3. **Nota bene** che *Tor Browser* non funziona su Windows XP e Vista.

4. Registrate il file **torbrowser-install-win64-9.5.3_en-US.exe** (questa è la versione in inglese (64 bit) di Tor Browser adatto alle versioni di Windows 7,8 e 10 ed è l'ultimo aggiornamento nel momento in cui redigiamo queste

istruzioni).

5. Noi usiamo la versione inglese e ne consigliamo l'uso perché, data la sua diffusione, garantisce meglio l'anonimato.

6. In questo breve manuale raccogliamo le informazioni minime indispensabili per iniziare a far funzionare TOR per la navigazione anonima su internet.

2. Installazione di Tor Browser

Avviate il programma "**torbrowser-install-win64-9.5.3_en-US.exe**". Vi si presenta una finestra per la selezione della lingua, vi viene proposta la stessa del vostro sistema operativo, vi consigliamo per motivi di sicurezza di scegliere l'inglese per nascondere meglio la vostra identità.
Si apre poi la finestra che vi permette di scegliere dove installare Tor Browser.
Installate il programma in una cartella che create sul disco interno del computer.
Alla fine dell'installazione vi appare una finestra in cui dovete deselezionate le due voci "Run Tor Browers" e "Add Start Menu & Desktop shortcuts". Deselezionando quest'ultima voce evitate che l'icona di Tor Browser appaia scrivania. Fate poi fate click sul bottone "Finish".
Per avviare Tor Browser aprite la cartella "Tor Browser". Nella cartella c'è l'icona con la "cipolla viola" (Start Tor Browser) che serve ad avviare Tor Browser. Facendo due click veloci su di essa si apre una finestra, in essa fate click sul bottone "Connect". Questa finestra vi appare solo la prima volta che avviate Tor Browser. La rivedrete eventualmente dopo che il programma Tor Browser si è interrotto in modo non corretto oppure nel caso non ci sia la connessione con la rete.
La prima volta è necessario aspettare alcuni minuti per l'avvio della navigazione.
A questo punto potete iniziare a navigare su internet in modo anonimo, **ma prima leggete i due capitoli che seguono**.

3. Perché siete anonimi utilizzando *Tor Browser*

Vi domanderete perché adesso che uso TOR sono anonimo. Lo siete perché tra il sito che visitate e il vostro computer si inserisce la rete TOR. L'indirizzo IP **(2)** che è quello che vi identifica quando vi connettete a internet serve a collegarsi ad un computer della rete TOR, poi le informazioni viaggiano in modo criptato tra i computer della rete ed alla fine giungono al sito che volete consultare attraverso l'ultimo computer della catena della rete TOR. Quindi venite identificati con l'IP di quest'ultimo computer. Inoltre i dati scambiati tra voi e la rete TOR e tra computer e computer delle rete TOR sono criptati con il metodo PGP **(3)** in modo da rendere impossibile risalire al vostro indirizzo IP. Solo l'ultimo computer decripta i comandi e i dati che inviate al sito che state consultando.

(2) L'indirizzo IP è un numero che viene assegnato ad ogni utente di internet e permette di identificarlo geograficamente. TOR si inserisce tra la vostra connessione e quella del sito finale: l'IP che vene riconosciuto dal sito consultato è differente dal vostro, inoltre i dati scambiati tra voi e la rete TOR sono criptati, in modo da rendere impossibile risalire al vostro indirizzo IP

(3) Per informazioni sul metodo PGP vedi:
http://www.nuovopci.it/comrapid/2019/05/Rapid_05.html

4. Avvertenze per la navigazione anonima

Prima di tutto un serie di avvertenze importanti.

Non dovete mai aggiungere estensioni e plug-in a Firefox. Se lo fate perdete l'anonimato.

Non dovete mai riempire moduli o richieste che contengano dati che si riferiscono a voi (lapalissiano, ma meglio ricordarselo).

Non dovete mai fare il copia e incolla da Firefox a Word o Open Office perché questi programmi quando ricevono i dati con il copia e incolla si collegano direttamente con internet per recuperarli e lo fanno senza usare TOR.
Se vi interessa un testo di una pagina internet, usate dal menu "File" la voce "Save Page As..." di Tor Browser. Quando si apre la finestra per indicare dove salvare il file, in basso nel campo "Type" impostate "Web Page Complete...". Il recupero dei dati avverrà esclusivamente via la rete di TOR. Salvate la pagina che vi interessa su una chiavetta USB. In seguito e solo dopo essersi scollegati da internet, potrete aprire la pagina salvata e recuperare testo e immagini facendo il copia e incolla o aprendo il file direttamente con Open Office o Word. **Notate Bene** che se siete inavvertitamente collegati ad internet e schiacciate un link presente nella pagina aperta con Word o Open Office, avviate la navigazione verso questo link attraverso il navigatore impostato come standard su Windows, cioè senza l'anonimato garantito da Tor Browser!

Quando consultare due webmail dello stesso provider dovete cambiate il vostro IP altrimenti qualcuno potrebbe dedurre un collegamento tra di esse e ricostruire la rete dei vostri contatti. Cambiate l'IP dopo aver consultato la prima webmail facendo click sul simbolo a forma di scopa a destra dello scudo, in alto nella finestra di Tor Browser. Tor Browser si chiude e si riapre ripulito di tutti i dati di navigazione precedenti: adesso potete consultare la seconda webmail.
Il cambiamento di IP appena descritto torna utile anche quando un sito non viene visualizzato: cambiando l'IP a volte si ristabilisce il corretto funzionamento del sito da consultare.

Attenzione! La navigazione con TOR è lenta, a volte lentissima. Non cercate di vedere filmati. Questa è una caratteristica della navigazione a cui vi dovrete abituare. Se inviate una email con un allegato molto grande, dovete avere pazienza. A volte vi sembrerà che il sistema si è incastrato.

Nota importante per la sicurezza dei dati:

Per non lasciare traccia dei vostri dati, dopo aver criptato o trasferito con l'operazione copia e incolla in un posto sicuro i dati da archiviare, usate **un programma per la cancellazione sicura (4)** per cancellare in modo definitivo i vostri file riservati rimasti sul computer. Solo con questo programma di cancellazione definitiva ogni traccia del vostro lavoro viene effettivamente cancellata.
Non dovete mai buttare nel cestino i file, altrimenti possono essere recuperati da virus, troiani e spioni. Cancellateli in modo definitivo con Eraser.
Non dovete mai fare operazioni di taglia / incolla da un disco (o chiavetta) a un'altro, perché il file originale viene messo nel cestino e non può più essere cancellato con Eraser. **Fate copia / incolla** del file su un altro supporto (chiavetta, disco esterno, ecc.) e poi cancellate con Eraser il file che è rimasto sul computer.

(4) di seguito due dei più diffusi programmi per la cancellazione sicura:
- Bleatchbit è reperibile alla pagina internet:
https://www.bleachbit.org/download/windows
- Eraser è reperibile alla pagina internet:
https://sourceforge.net/projects/eraser/

5. La posta anonima con TOR

Per l'invio e la ricezione della posta in modo anonimo con Tor Browser non si possono usare programmi tipo Outlook. Bisogna imperativamente usare le Webmail, cioè caselle email consultabili attraverso il navigatore Tor Browser.
Naturalmente bisogna creare una casella nuova e non riconducibile a voi.
Il principale problema che vi si presenterà sarà dato dal fatto che i principali provider di posta elettronica chiedono al momento dell'attivazione della casella un numero di cellulare, quindi provider tipo Yahoo, Google ecc. non possono essere utilizzati a questo scopo. Altri invece riconoscono che usate TOR e non permettono l'apertura di un email.
Nel momento in cui scriviamo il migliore sistema per creare una casella email è disponibile sul sito di autistici.org al seguente link: https://www.autistici.org/services/
Informazioni sul altri siti che offrono la possibilità di aprire in modo anonimo le webmail si trovano ai seguenti indirizzi:
https://hacker10.com/other-computing/list-of-the-best-free-webmail-privacy-services/
http://mail2tor2zyjdctd.onion/register.php - Si accede solo utilizzando TOR. Potete aprire istantaneamente due email per scambiarvi messaggi (potete inviare e ricevere messaggi solo tra le caselle dello stesso provider nome_casella1@mail2tor.com a nome_casella2@mail2tor.com).

2. **ATTENZIONE - Basta una sola sessione di consultazione di una email senza l'uso di TOR per lasciare una traccia della vostra identità!**

3. **Un sistema alternativo alle email per la comunicazione anonima è we.riseup.net**
Non è una casella email, è un spazio internet dove si depositano i documenti. Naturalmente li dovete criptare **(5)** prima di depositarli se volete salvare baracca e burattini. I corrispondenti devono controllare regolarmente il vostro spazio e ritirare il documento depositato. L'apertura dello spazio è immediata, nessuna necessità di dati.
Per aprire lo spazio su we.riseup.net, il modulo da compilare si trova all'indirizzo:
https://we.riseup.net/account/new .
NMB (Nota molto bene): l'email richiesta nel modulo è facoltativa, non occorre indicarla. Appena compilato il modulo lo spazio di scambio è subito disponibile.

(5) Per criptare i documenti dovete usare il sistema **PGP**. Per Windows il programma lo trovate al seguente indirizzo:
http://www.gpg4win.org/download.html
Istruzioni sintetiche per il l'utilizzo del sistema PGP le trovate in:
http://www.nuovopci.it/comrapid/2019/05/Rapid_05.html

6. Usate un antivirus e aggiornate regolarmente Windows

1. **È assolutamente necessario avere sempre un antivirus aggiornato**. Su Windows 10 quello fornito di sistema è sufficiente.
2. **Dovete eseguire regolarmente l'aggiornamento di Windows** perché gli spioni approfittano delle falle di sicurezza. Se non aggiornate Windows stendete un tappeto rosso a tutti gli spioni e le polizie!!!

7. Ricordatevi che TOR protegge il vostro anonimato, non le informazioni che inviate

Attenzione! Il sistema TOR protegge l'identità di chi invia o riceve un'informazione, ma non le informazioni che vengono inviate. Chi spia può intercettare il vostro messaggio. Se inviate: "L'assalto al Palazzo d'Inverno è domani alle 12.30", non aspettatevi nulla di buono. L'esempio è volutamente imbecille, proprio per non farvi scordare questa caratteristica di TOR e perché dovete imparare ad usare il sistema PGP **(vedi la nota 5)** per criptare i dati da inviare.

8. Aggiornamento automatico di Tor Browser

Dalla versione 4.0.3 in poi di Tor Browser è stato introdotto l'aggiornamento automatico del programma, se usate TOR saltuariamente all'avvio il programma automatico di aggiornamento provvederà a verificare se esiste una nuova versione e nel caso aggiornare il programma sul vostro computer.

È necessario usare sempre la versione più aggiornata di Tor Browser: in ogni aggiornamento sono migliorate le difese contro gli spioni ed eliminati i difetti che possono compromettere l'anonimato.

Buon lavoro compagni e sinceri democratici!