L'anonimato e la privacy in internet non sono così immediate. Mentre navighiamo, scarichiamo la posta o visitiamo qualche Social Network molte informazioni personali o comportamenti vengono lette, collezionate e utilizzate al bisogno per indagini di mercato, pubblicità o peggio.

Il problema lo abbiamo già affrontata presentando in diversi articoli soluzioni ed accorgimenti tesi a proteggere la nostra privacy. Vediamo una nuova soluzione che potrebbe risolvere molti dei nostri problemi di anonimato e privacy tutti assieme.

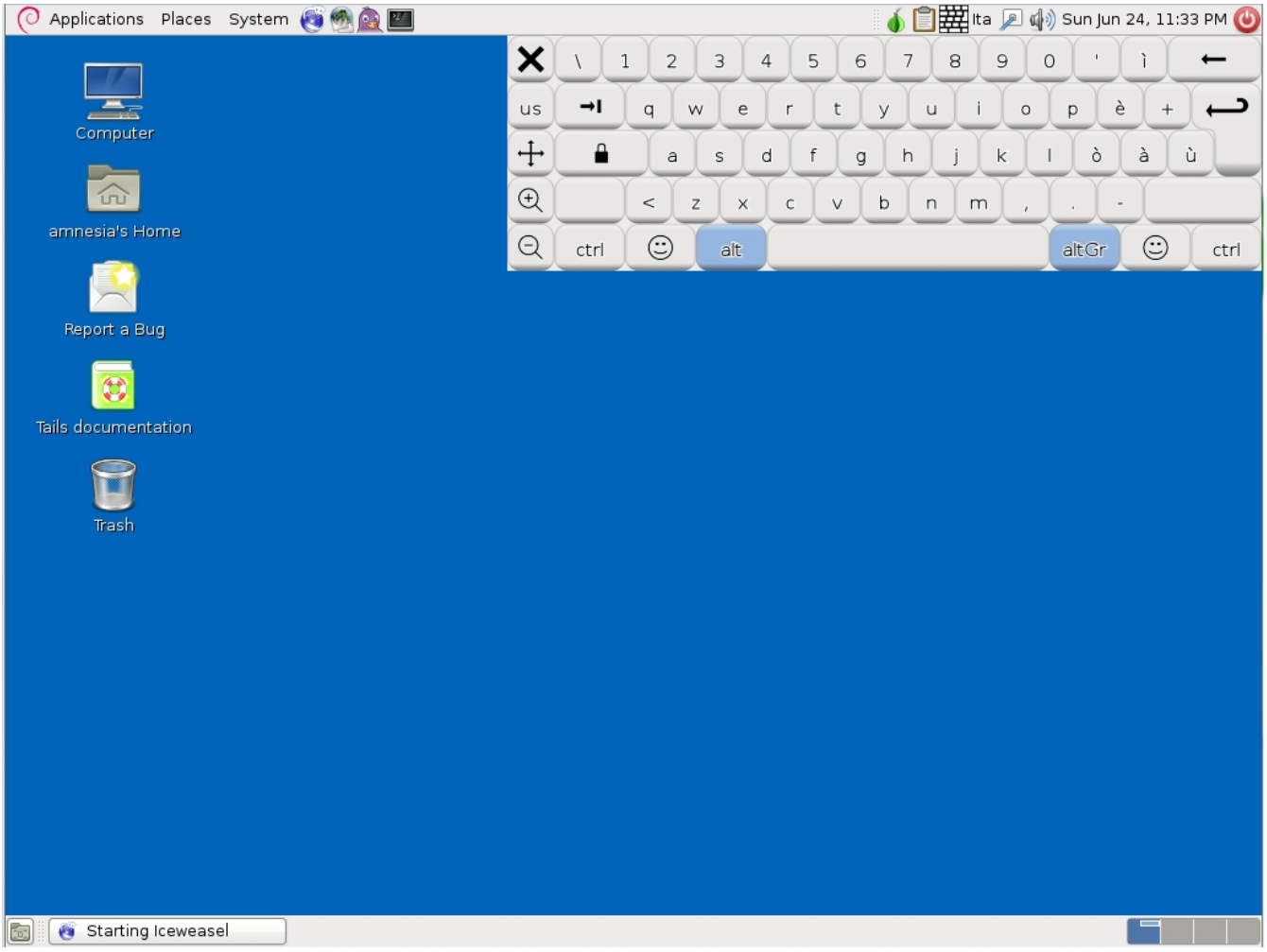
Esiste una nuova distribuzione linux concepita e sviluppata per proteggere l'anonimato dei propri utenti: Tails . Tails (o “The Amnesic Incognito Live System”) è stata progettata per proteggere la privacy e l'anonimato dei propri utenti basandosi su tre concetti fondamentali:

Usare internet anonimamente Tutte le applicazioni installate in Tails che richiedono il collegamento ad internet sono sono volutamente configurate per utilizzare la rete Tor (vedi: “ Web Privacy: Tor Project ”). La rete Tor garantisce totalmente anonimato e la irrintracciabilità dell'utente.

Non lasciare traccie

Tails è una distribuzione linux live e non richiede installazione sul sistema che lo ospita per la sua esecuzione. Grazie a tale modalità non lascia nessuna informazione sul computer che lo ha “ospitato”. Inoltre, può essere facilmente installata su un CD Rom o su una Pendrive ed un utente può portarla sempre con se ed usarla all'occorrenza.

Per fare un esempio di quanto possa essere avanzato il livello di sicurezza di questa distribuzione, di default è attivata la tastiere virtuale (Florence Virtual Keyboard). La tastiera virtuale impedisce che applicazioni molto avanzate o eventuali dispositivi fisici (keylogger hardware), precedentemente installate sulla macchina ospitante Tails, possano intercettare i tasti digitati dalla tastiera.

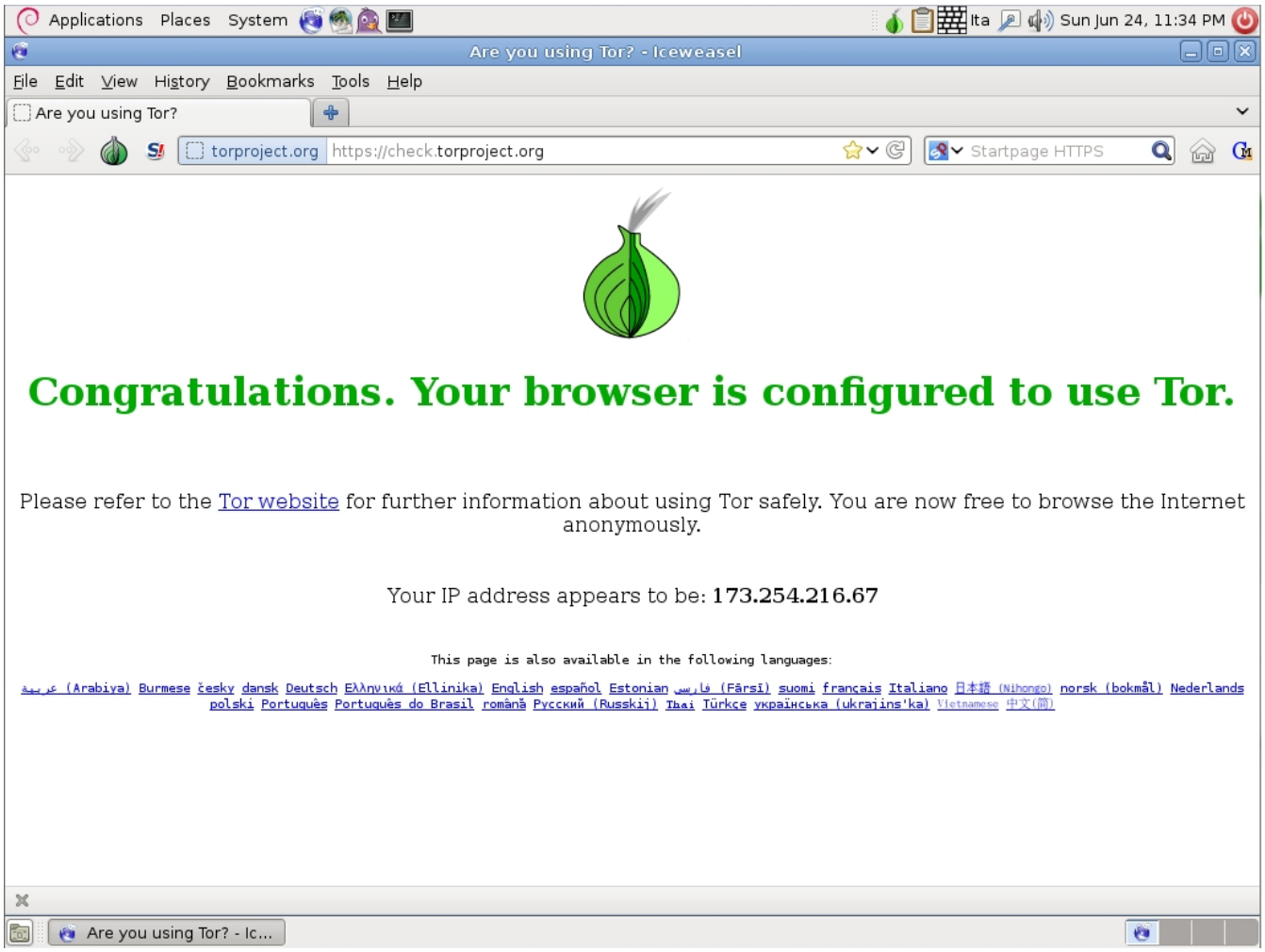


Crittografa Tutto

In Tails sono disponibili i migliori strumenti applicativi messi a disposizione dalla comunità open source per crittografare dischi, email, archivi, messaggi istantanei, etc. Qualsiasi messaggio trasmesso da una applicazione di Tails è, per definizione, cifrata. Per esempio, il browser Iceweasel (la versione ottimizzata di Firefox per Debian), oltre ad essere già anonimo grazie alla rete Tor, nelle connessioni in modalità sicura HTTPS cifra le informazioni automaticamente attraverso una estensione già installata e configurata denominata HTTPS Everywhere .

Le email ed i documenti vengono cifrati attraverso lo standard de facto OpenPGP basato su

algoritmi di cifratura molto evoluti.



Descrizione della distribuzione

Tails si basa sulla nota distribuzione Linux Debian 6.0.4 (su cui si basa anche Ubuntu) ed è libera e gratuita.

Il desktop è lo Gnome di Debian (molto semplice e lineare) con installato un tema standard senza troppi elementi grafici che tenderebbero ad appesantire l'esecuzione o a non farlo funzionare su sistemi obsoleti (i requisiti minimi sono un IBM PC compatibile: supporta Intel x86-based, AMD64 o Intel EM64T).

Il software in dotazione è di tutto rispetto. Di default è installato l'intera suite di OpenOffice (la 3.2.1 e non l'ultima versione 3.4), alcuni programmi per la grafica ed il multimedia (Gimp, InkScape, Audacity, ScribusNG, etc) e tutte le applicazioni minime per il collegamento ad internet (Iceweasel come browser, Pidgin per l'instant messaging e Claws per la posta elettronica).

Molto interessanti sono le utility legate alla sicurezza (Tor, Vidalia, TrueCrypt, Etc.). Sono già tutte installate, configurate e pronte all'uso. Oltre a le funzionalità su menzionate, spicca anche una funziona “Wipe” che permette la cancellazione fisica e permanente dei dati dal proprio disco rigido per impedirne un eventuale recupero “malizioso”.

La distribuzione è live e non prevede installazione (se non voluta dall'utente). Per utilizzarla è sufficiente scaricare dal sito la copia del disco di Tails (l'ultima versione disponibile è la 0.12) e masterizzarla su un CD.

La procedura di installazione su chiavetta può essere fatta direttamente dal CD autopartente precedente generato. Durante la sua esecuzione, occorre richiamare la procedura automatica “Tails Live USB Creators” dal menu “Applications->Tails”.

Nel caso non possiate masterizzare un CD, potete seguire la procedura descritta nell'articolo “ Un PC su una Pendrive... ” dopo aver scaricato l'immagine ISO di Tails dal link .

La documentazione online è ricca ed esaustiva e, per i punti di approfondimento, rimanda ai siti principali esterni al progetto Tails.
L'unica pecca riscontrata è che Tails non supporta l'Italiano (se non per la tastiera e le configurazioni di base di localizzazione) e nessuno dei menu è tradotto nella nostra lingua.

Per chi viaggia ed utilizza computer in condizioni “pericolose” (Hall di albergo, Internet Center, etc) Tails è sicuramente da provare e fidarsi è bene, ma non fidarsi è meglio!

(25/06/2012)