به کمک تُر و وردپرس، ناشناس وبلاگ بنویسید

مقدمه:

یکی از بزرگترین مزیت‌های کار با Global Voices این بود که شانس همکاری با افرادی را داد که به جای اینکه توسط قدرت و نیروهای امنیتی ساکت شوند، به راحتی حرف می‌زدند. من با عده‌ای از نویسندگان که دوست داشتند در مورد مسائل شخصی و سیاست بر روی وب بنویسند کار می‌کردم، اما آنها احساس می‌کردند که نمی‌توانند به صورت آنلاین در مورد ایده‌ها و عقایدشان بنویسند، چون ممکن است که رهگیری و شناسایی شوند. این نویسندگان که شامل فعالان حقوق بشر از ملیت‌های مختلف بودند، به افراد کمک می‌کردند تا از سرکوب‌هایی که در کشورهای مختلف صورت می‌گیرد، گزارش تهیه کنند.

مدتی قبل، مقاله‌ای تحت عنوان «راهنمایی جامع برای نوشتن وبلاگ به صورت ناشناس» را در Global Voices منتشر کردم که شامل روش‌های مختلفی برای وبلاگ‌نویسی به صورت ناشناس بود. و پس از آن چندین کارگاه آموزشی در نقاط مختلف جهان برگزار کردم که در آن با ترکیبی از ابزارهای مختلفی مانند تُر، وردپرس و حساب‌های رایگان ایمیل، وبلاگ‌نویسی را با بیشترین درجه‌ی ناشناس بودن، آموزش می‌دادم. راهنمایی که در ادامه خواهید خواند، راه حل‌های دیگر را نفی نمی‌کند، بلکه راهی است که شامل جزئیاتی دقیق است.

اگر می‌خواهید این راهنما را به سرعت بخوانید و یا اگر نمی‌خواهید بدانید که به چه دلیل این کار را باید انجام دهید، شما می‌توانید قسمت‌های «چرا» در این راهنما را نخوانید.

اگر در جایی از این راهنما شما نکته‌ی غیرشفاف و یا اشتباهی دیدید، لطفا من را از طریق Global Voices مطلع کنید. این راهنمای تحت لیسانس Creative Commons 2.5 Attribution و بدین معنا است که شما می‌توانید به صورت رایگان آن را چاپ و به فروش برسانید، اگر شما فکر می‌کنید که می‌توانید از این طریق درآمد و بازاری داشته باشید.

مسئولیت:

اگر شما تمام مراحل را به صورت دقیق اجرا کنید، شانس شناسایی شما از طریق فعالیت‌های اینترنتی‌تان توسط راه‌های تکنیکی مانند شناسایی به وسیله‌ی دولت و یا نیروهای امنیتی به کمک رهگیریتان در سرویس‌های ارائه دهنده‌ی خدمات اینترنتی (ISP) به میزان بسیار زیادی کاهش پیدا می‌کند. متاسفانه، من نمی‌توانم ضمانت کنم که این روش به طور کاملا درست و قابل اجراست و شما را می‌تواند از همه‌ی چیز محافظت کند.
این روش شما را مورد محافظت در برابر دیگر تکنیک‌های شناسایی قرار نمی‌دهد، مانند نصب نرم‌افزارهایی بر روی رایانه شما که سوابق کاری شما را ضبط و ثبت کنند یا روش‌های نظارت سنتی مانند تحت نظر گرفتن شما از طریق تماشای صفحه‌ی نمایشگرتان توسط دوربین. در حقیقت اکثر مردم با طرز نوشتن خود، قابل شناسایی هستند، به طور مثال آنها با استفاده از تکه کلام‌هایی که در تمام نوشته‌هایشان استفاده می‌کنند، باعث می‌شوند که شناسایی آنها راحت‌تر باشد. و من نمی‌توانم به این افراد کمک کنم مگر اینکه به آنها بگویم مراقب و هوشیار باشند. برای اینکه بدانید، چگونه مراقب و هوشیار باشید، خواند مقاله‌ای با عنوان «چگونه در امنیت وبلاگ بنویسید» را پیشنهاد می‌دهم.

و حالا اصل موضوع:

1- نوشتن از رایانه‌های عمومی (مشترک)
اگر شما برای نوشتن از رایانه‌های عمومی یا مشترک (مانند کافی‌نت‌ها) استفاده می‌کنید یا قادر نیستید که نرم‌افزاری بر روی رایانه نصب کنید، لطفا مراحل زیر را بدون نیاز به نصب کردن هیچ نرم‌افزاری دنبال کنید تا بسته‌ی مرورگر تُر(Tor Browser Bundle) را نصب کنید.

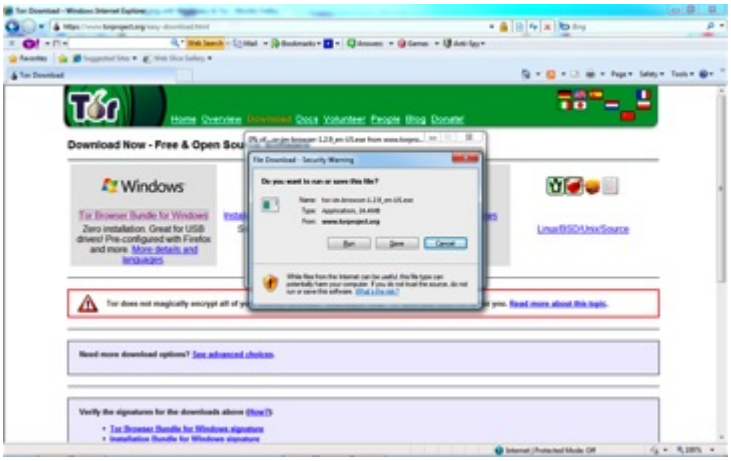
اما اگر شما از رایانه‌ی شخصی استفاده می‌کنید و می‌توانید بر روی رایانه‌ی خود نرم‌افزار نصب کنید، به بخش (2) مراجعه کنید.

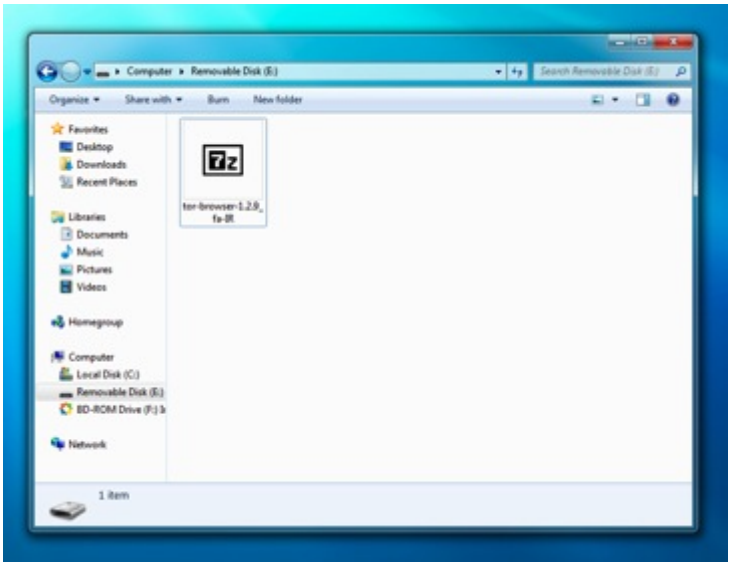
نصب بسته‌ی Zero بر روی ویندوز (برای هرگونه درایوهای قابل حمل)

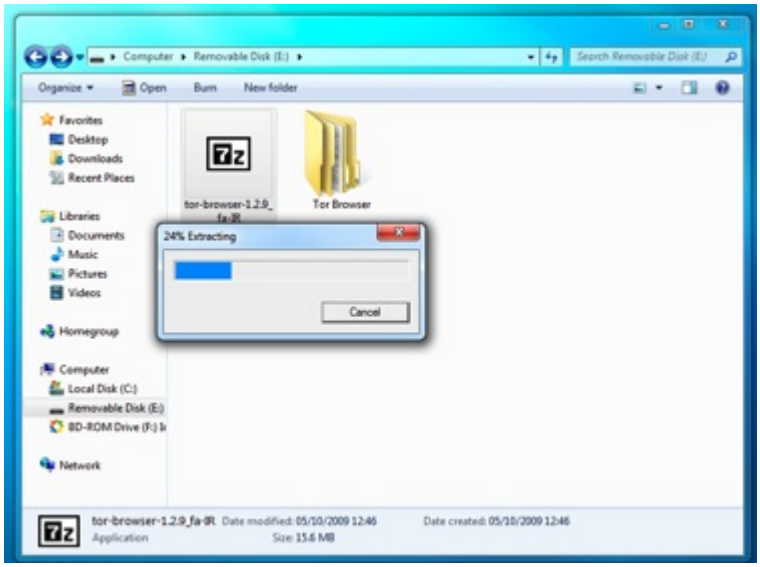
ما پیشنهاد می‌دهیم که شما بسته‌ی Zero را برای ویندوز دانلود کنید، که یک پیش‌نیاز عالی برای بسته‌ی نرم‌افزاری تُر (Tor) است، و شامل مرورگر قابل حمل فایرفاکس است که می‌توان به راحتی آن را به کمک حافظه‌های قابل حمل مانند کارت‌های SD، هارد دیسک‌ها، کارت‌های حافظه‌ی فلش، جا به جا کنید. مرورگر تُر نسخه‌ی متن باز قابل حملی است که توسط پروژه‌ی تُر ایجاد شده است. این مرورگر، نسخه‌ی سفارشی فایرفاکس است که در آن، ویدالیا (Vidalia)، فراخوان پروکسی http که پولیپو (Polipo) خوانده می‌شود، فایرفاکس، و دکمه‌ی تُر، نصب شده است. این بسته برای قرار گرفتن در حافظه‌های یواس‌بی (USB) طراحی شده است که شما می‌توانید به تُر در رایانه‌های عمومی که اجازه‌ی نصب برنامه‌ای در آنها وجود ندارد، دسترسی داشته باشید.

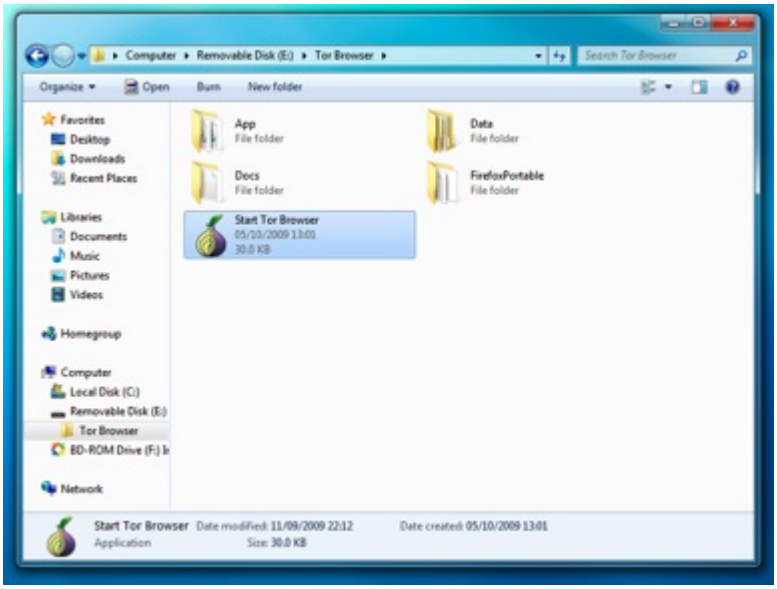
الف) دانلود کردن بسته‌ی مرورگر تُر. ابتدا بسته را براساس زبان انتخابی خود، از وب‌سایت پروژه‌ی تُر بر روی رایانه خود دانلود و ذخیره می‌کنید. سپس حافظه‌ی یواس‌بی را بر روی رایانه نصب کرده و بسته‌ی مرورگر تُر را بر روی آن کپی می‌کنید. حال به کمک حافظه‌های یواس‌بی و هر ویندوزی که بر روی رایانه نصب است، می‌توانید با وارد شدن به حافظه‌ی یواس‌بی، به مرورگر حفاظت‌شده‌ی تُر دسترسی داشته باشید. بر روی رایانه‌ی عمومی، مرورگر وب دیگری را استفاده نکنید. حافظه‌ی یواس‌بی را نصب کنید، فایل اجرایی (filesystem) را از حافظه‌ی یواس‌بی پیدا کرده و بر روی دسکتاپ قرار دهید و سپس بر روی Start Tor Browser.exe دو بار کلیک کنید. پنجره‌ی ویدالیا (Vidalia) به سرعت ظاهر خواهد شد.

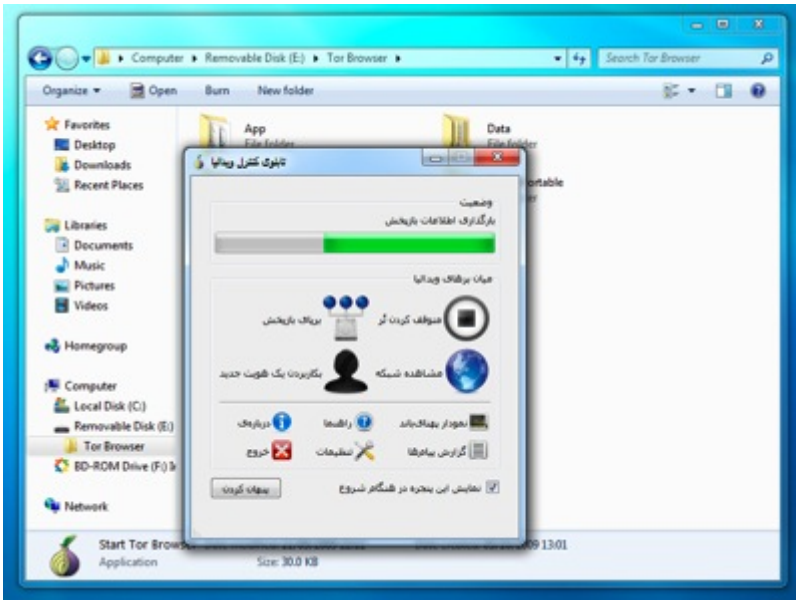
به خاطر داشته باشید که شما می‌توانید بسته‌ی مرورگر تُر را از وبسایت پروژه‌ی تُر دانلود کنید و زبان مورد علاقه‌ی خود را از صفحه‌ی دانلود بسته‌ی مرورگر تُر دانلود کنید.

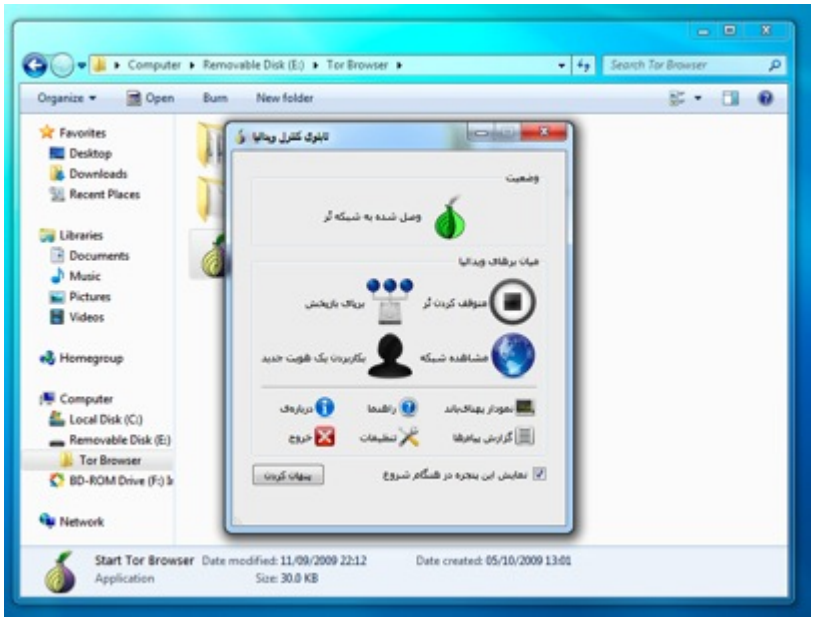










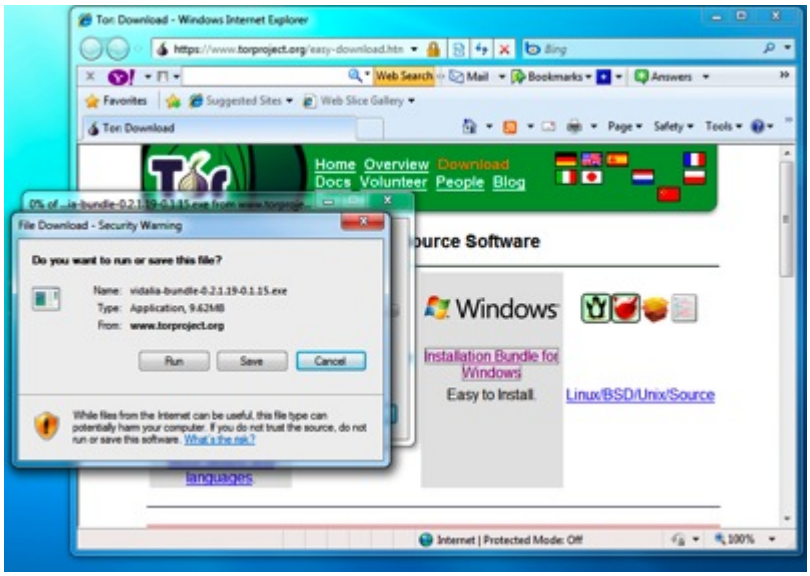


ب) فایل را بر روی یواس‌پی کپی کنید، پوشه‌ی Tor Browser را باز کنید و بر روی Start Tor Brower کلیک کنید. بعد از آن اتصال به شبکه‌ی تُر انجام می‌شود و بعد از فعال شدن تُر، به صورت خودکار مرورگر فایرفاکس باز می‌شود و صفحه‌ی تست تُر به شما پیام «مژده. شما (احتمالا) در حال استفاده از تُر می‌باشید» را نشان خواهد داد. در غیر این صورت، شما پیام «متاسفانه شما از تُر استفاده نمی‌کنید. اگر شما از نرم‌افزار تُر استفاده می‌کنید، لطفا به وبسایت تُر مراجعه کنید و دستورالعمل تنظیمات نرم‌افزار تُر را با دقت بخوانید.»

2- نوشتن از رایانه شخصی‌تان
اگر شما بخواهید که از رایانه‌ی شخصی خود وبلاگ بنویسید، حتما می‌توانید بر روی آن نرم‌افزار نصب کنید. برای این کار مراحل زیر را پی‌گیری کنید:
مرحله اول: تغییر آی‌پی
همه‌ی رایانه‌های متصل به اینترنت به صورت اختصاصی یا مشترک دارای یک آدرس آی‌پی هستند. این آدرس‌ها شبیه آدرس‌های محل زندگی نیستند، اما می‌توانند سیستم‌های مدیریتی هوشیار را به آدرس محل زندگی شما راهنمایی

کنند. به خصوص، اگر شما از یک ارائه‌دهنده‌ی خدمات اینترنتی (ISP) استفاده می‌کنید، در اغلب اوقات می‌توان از طریق آی‌پی، شماره تلفن اتصال شونده را در یک زمان خاص که از آن آی‌پی درخواستی شده است را پیدا کرد. بنابراین ما باید قبل از هر کاری، آی‌پی خود را تغییر دهیم.
کاری که باید شما برای نوشتن وبلاگ از محل کار یا خانه‌ی خود انجام دهید این است که:
الف) نصب فایرفاکس. فایرفاکس را از وبسایت موزیلا دانلود و بر روی رایانه‌ای که می‌خواهید از آن وبلاگ بنویسید، نصب کنید.

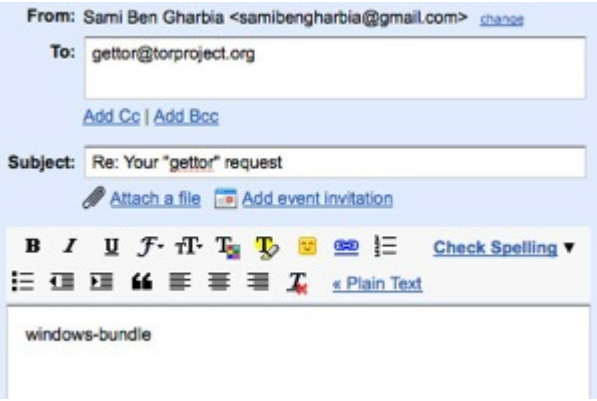
چرا؟
اینترنت اکسپلورر (Internet Explorer) دارای حفره‌های امنیتی فاحشی است که می‌تواند امنیت شما را به خطر بیاندازد. این حفره‌ها از مدت‌های طولانی بر روی اینترنت اکسپلورر وجود داشته است. این مرورگر در مقابل حملات نرم‌افزارهای جاسوسی و یا ویروس‌هایی که ممکن است در هنگام دانلود یک فایل وجود داشته باشند، بسیار ضربه‌پذیر است. همچنین، بسیاری از ابزارهای حریم خصوصی که منتشر شده‌اند بر روی فایرفاکس کار می‌کنند، مانند Torbutton، که ما در مراحل بعدی از آن استفاده می‌کنیم.
ب) نصب تُر. می‌توانید این برنامه را از وب‌سایت تُر دانلود کنید. اگر وب‌سایت تُر در کشور شما فیلتر شده است، آدرس‌های بسیار زیاد دیگری وجود دارند که شما می‌توانید از آنها برای دانلود استفاده کنید. شما می‌توانید با جستجوی «site:torproject.org mirrors» در موتور جستجوی گوگل و به کمک ذخیرساز گوگل (google cache) بسیاری از صفحات کمکی را مشاهده کنید. آخرین نسخه‌ی پایدار را براساس سیستم عامل رایانه‌یتان انتخاب و آن را بر روی دسکتاپ خود ذخیره کنید. سپس مراحل را براساس دستورالعملی که در فایل دانلود شده وجود دارد، پشت سر بگذارید. شما دو بسته‌ی نرم‌افزاری نصب خواهید کرد که نیاز به چند تغییر در تنظیمات (Setting) این برنامه‌ها دارید.



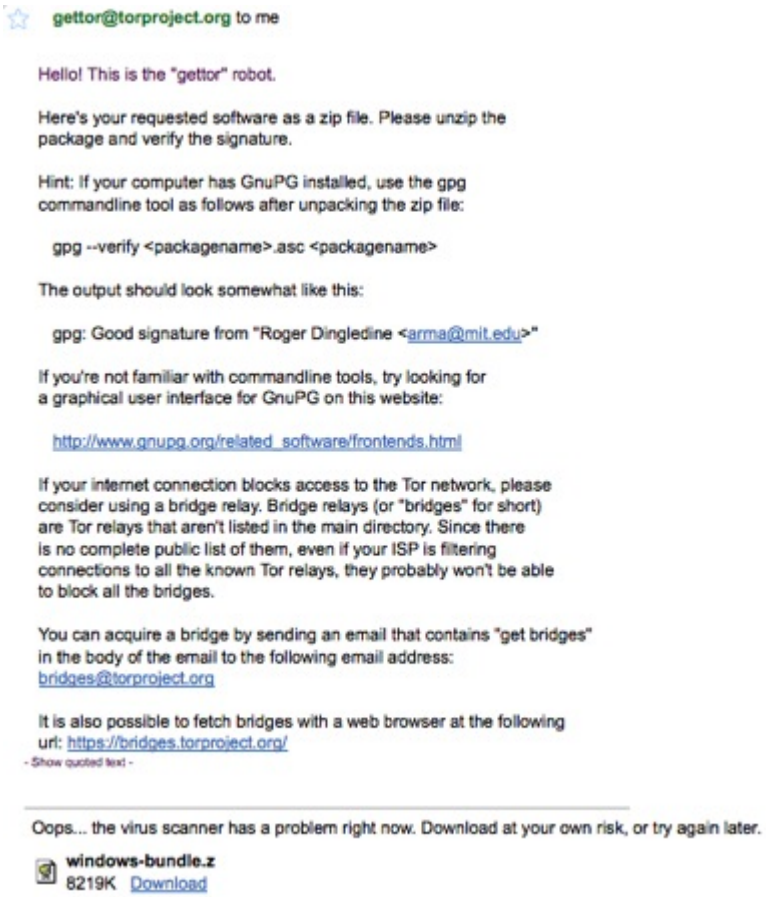
اگر اتصال اینترنت شما به وب‌سایت تُر بسته بود، می‌توانید بسته‌ی خود را به وسیله‌ی ایمیل از ربات gettor به آدرس gettor [At] torproject [DOT] org دریافت کنید. به خاطر داشته باشید، ایمیل‌هایی که به gettor@torproject.org فرستاده می‌شود، باید از سرویس جی‌میل فرستاده شوند، در غیر این صورت هیچ پاسخی دریافت نخواهید کرد. نام یکی از بسته‌های زیر را هم باید انتخاب کنید و در قسمت متن ایمیل (Body) بنویسید:

- tor-im-browser-bundle
- windows-bundle
- panther-bundle

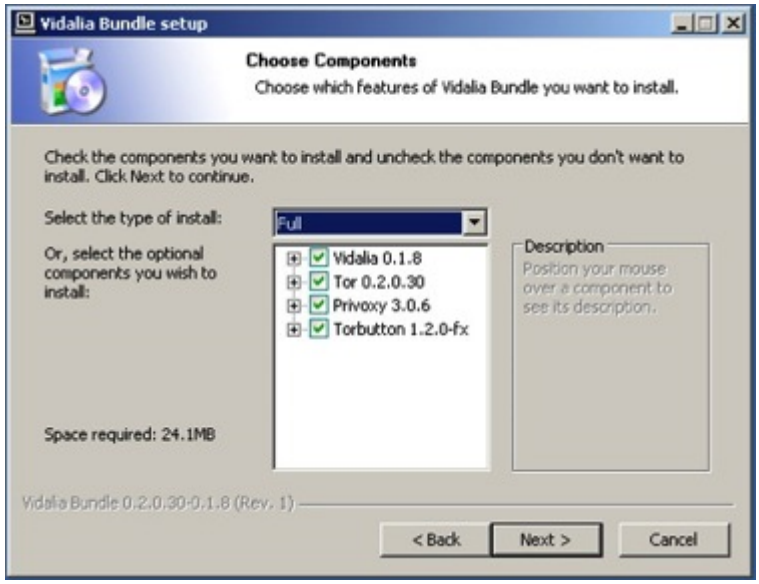
- tor-browser-bundle
- source-bundle
- tiger-bundle

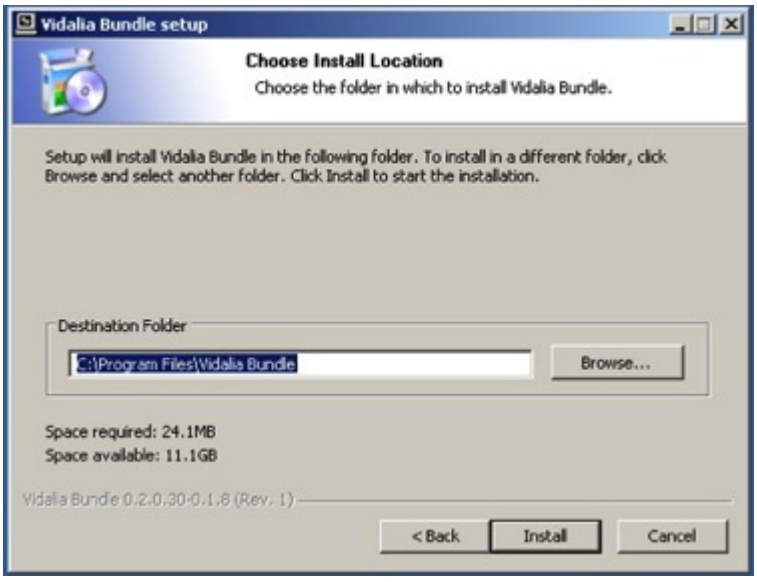


مدت کوتاهی بعد از اینکه ایمیل فرستاده شود، ایمیلی از طرف ربات «Gettor» دریافت می‌کنید که در آن نرم‌افزار درخواستی شما به صورت فایل فشرده (Zip) فرستاده است.



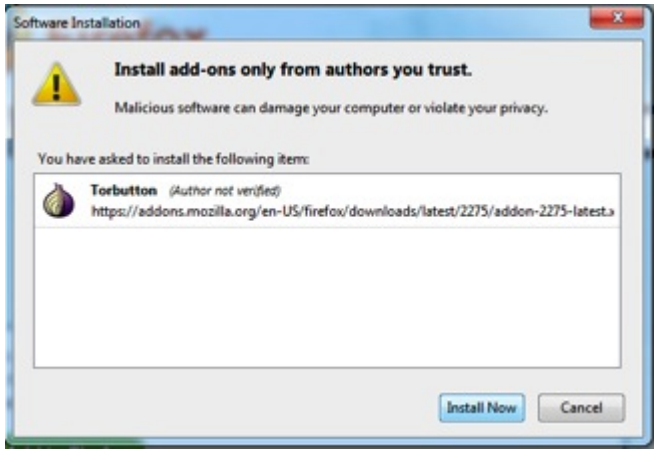

Vidalia Bundle setup
Welcome to the Vidalia Bundle Setup Wizard
This wizard will guide you through the installation of Tor, Vidalia, Privoxy, and Torbutton.
Tor is a system for using the Internet anonymously, helping you anonymize Web browsing and publishing, instant messaging, IRC, and more. Vidalia 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


Vidalia Bundle setup
Choose Install Location
Choose the folder in which to install Vidalia Bundle.
Setup will install Vidalia Bundle in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Vidalia Bundle
Browse...
Space required: 24.1MB
Space available: 11.1GB
Vidalia Bundle 0.2.0.30-0.1.8 (Rev. 1)
< Back
Install
Cancel

چرا؟

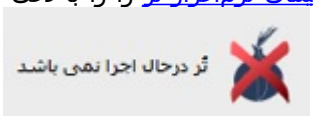
تُر یک شبکه‌ی با کیفیت از سرورهای پروکسی است. سرورهای پروکسی درخواست صفحه‌ی وب شما را به صورت پنهانی انجام می‌دهند و این بدان معنا است که سرور وب نمی‌تواند آی‌پی درخواست کننده‌ی صفحه‌ی وب را ببیند.
زمانی که شما به تُر دسترسی دارید، از سه سرور مختلف پروکسی برای فراخوانی هر صفحه‌ی وب استفاده می‌کنید. صفحات در حین انتقال بین سرورها رمزگذاری می‌شوند و اگر یک یا دو سرور به صورت زنجیروار با یکدیگر مقایسه شوند، تشخیص اینکه شما چه صفحاتی را فراخوانی و یا پست کرده‌اید، بسیار سخت خواهد بود.
تُر نرم‌افزار دیگری به نام Privoxy را هم نصب می‌کند که امنیت تنظیمات (Setting) مرورگر شما را افزایش می‌دهد، دسترسی کوکی‌ها و دیگر قسمت‌هایی را که می‌توان شما را با آنها رهگیری کرد را می‌بندد و به راحتی تمام آگهی‌هایی که بر روی صفحات وب هست را نیز فیلتر می کند.
پ) نصب بسته‌ی تُر به کمک Torbutton **Torbutton** که یک افزونه‌ی برای فایرفاکس است و به راحتی می‌توانید آن را نصب کنید. برای این کار بر روی Install Now کلیک می‌کنید، فایرفاکس شما راه‌اندازی مجدد (Restart) می‌شود و کار تمام است.



چرا؟
فعال کردن تُر به صورت دستی بدین معنا است که باید به یاد داشته باشید که تنظیمات مرورگر خود را برای استفاده از سرور پروکسی تغییر بدهید. در این کار چندمرحله‌ای، برخی زمان‌ها افراد یادشان می‌رود که این کار را انجام دهد. Torbutton این کار را تنها با یک کلیک انجام می‌دهند و به شما یادآوری می‌کند که آیا از Tor استفاده می‌کنید یا خیر.
در حقیقت به دلیل اینکه تُر از سه پروکسی مختلف استفاده می‌کند تا به سرور وب برسد، ممکن است سرعت وبگردی شما را کاهش می‌دهد. برخی افراد- از جمله من- از تُر تنها در مواردی استفاده می‌کنم که برایم تغییر شناسایی با اهمیت باشد، در غیر این صورت آن را غیرفعال می‌کنم.

ت) فعال کردن تُر در فایرفاکس و تست آن. زمانی که تُر فعال است، به این سایت بروید (https://check.torproject.org/). بعد از کلیک کردن، اگر شما این پیام را دریافت کردید که به شما می‌گوید، «مژده. شما (احتمالا) در حال استفاده از تُر می‌باشید. لطفا برای اطلاعات بیشتر در مورد استفاده امن‌تر از تُر، به وب‌سایت تُر مراجعه کنید.»، یعنی همه چیز را درست نصب شده است و شما آماده‌اید که به مرحله‌ی بعد بروید.

در غیر این صورت، شما پیام «متاسفانه شما از تُر استفاده نمی‌کنید. اگر شما از نرم‌افزار تُر استفاده می‌کنید، لطفا به وب‌سایت تُر مراجعه کنید و دستورالعمل تنظیمات نرم‌افزار تُر را با دقت بخوانید.»

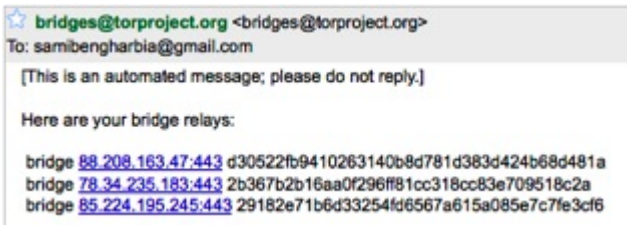


چرا؟
وقتی که می‌بینید یک نرم‌افزار که نصب کرده‌اید، کار می‌کند، همواره یک احساس خوب ایجاد می‌شود، مخصوصا زمانی که کار مهمی مانند آنچه تُر انجام می‌دهد را بکند. تُر صفحه‌ای که می‌خواهید به آن دسترسی داشته باشید را بررسی می‌کند که از چه آی‌پی و از کجا این درخواست صورت گرفته است. اگر این درخواست از ندهای تُر (Tor node) باشد، تُر به درستی کار می‌کند و آی‌پی شما را تغییر می‌دهد- اگر نه، مشکلی وجود دارد و شما باید سعی کنید، بفهمید چرا تُر به درستی کار نمی‌کند.

مشکل چیست اگر تُر هرگز وصل نشد؟
اگر شما مشکلی در اتصال به شبکه‌ی تُر دارید، باید قسمت سوالات متداول را بخوانید. اگر در اتصال اینترنت شما به شبکه‌ی تُر دسترسی نداشته باشید و آیکون ویدالیا در قسمت System Tray به رنگ زرد بود، ممکن است شما بتوانید از Bridge relays استفاده کنید.

> Bridge relays (یا به صورت خلاصه Bridge) تقویت‌کننده‌های تُر هستند که در پوشه‌ی اصلی تُر وجود ندارند. تاکنون هیچ لیست کاملی از آن‌ها به صورت عمومی ارائه نشده است، هرچند برخی از ارائه‌دهندگان خدمات اینترنتی تمام ارتباطاتی که به عنوان تُر شناخته می‌شوند را فیلتر می‌کنند، اما آنها قادر نیستند که تمام Bridgeها را ببندند. اگر دسترسی شما به شبکه تُر معلق و بسته باشد، شما ممکن است بخواهید که از Bridge استفاده کنید.

شما می‌توانید به کمک فرستادن ایمیل، Bridge را دریافت کنید. برای این کار از حساب خود در جی‌میل، ایمیلی به آدرس bridges@torproject.org می‌فرستید که در متن آن عبارت «get bridges» نوشته شده باشد. مدت کوتاهی بعد، به صورت خودکار پیامی دریافت خواهید کرد که در آن Bridge قرار دارد. علاوه بر این می‌توانید از طریق آدرس https://bridges.torproject.org هم آن را دریافت کنید.
صفحه‌ی کنترل (Control Panel) ویدالیا را باز و مسیر Setting> Network را طی کرده و بر روی My ISP blocks connections to the Tor network کلیک کنید. هر آدرس Bridge را در قسمت Add a Bridge اضافه کرده و سپس بر روی علامت + کلیک کنید.



مرحله دوم: ایجاد یک حساب ایمیل امن و مشکل برای رهگیری

اکثر سرویس‌های وب- شامل سرویس‌های میزبانی وبلاگ- نیاز به آدرس ایمیل دارند تا بتوانند با کاربرانشان در ارتباط باشند. برای هدف ما، این آدرس ایمیل نمی‌تواند اطلاعاتی را داشته باشد که بتوان با آن هویت ما را شناسایی کرد، مانند آدرس آی‌پی که برای وارد شدن به حساب ایمیل از آن استفاده می‌کنیم. این بدان معناست که ما نیاز به یک حساب جدید داریم که از طریق تُر آن را باز کنیم، و مطمئن شویم که هیچگونه اطلاعاتی مانند نام، آدرس و... به گونه‌ای که به ما مربوط شود، وجود ندارد. شما نباید از حساب ایمیلی که وجود دارد استفاده کنید- این بسیار مهم است که شما حسابی را که باز می‌کنید با آدرس آی‌پی ناشناس باشد و سرویس ارائه‌دهنده‌ی ایمیل آدرس آی‌پی شما را به صورت نادرست ثبت کند.

الف) انتخاب سرویس ارائه‌دهنده‌ی ایمیل. ما به شما Riseup.net و یا جی‌میل را پیشنهاد می‌کنیم، اما اگر به صورت متداوم از تُر استفاده می‌کنید، شما می‌توانید از یاهو یا هات‌میل هم استفاده کنید. همچنین می‌توانید سریع و رایگان در fastmail.fm هم حساب داشته باشید.

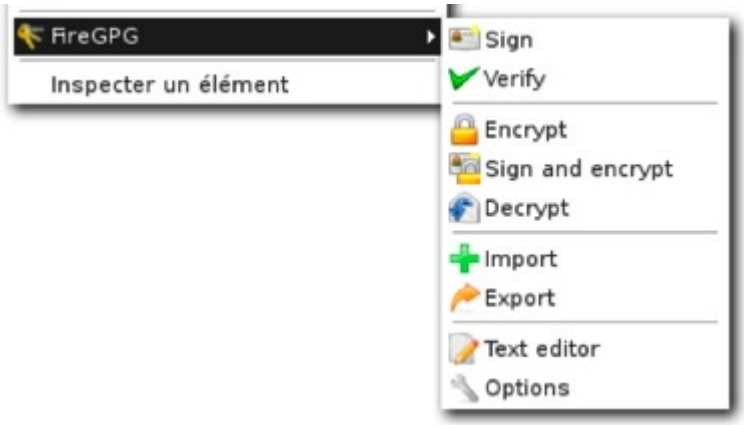
چرا؟

ایمیل تحت وب (Webmail) بهترین روش برای ایجاد ایمیل است و شما می‌توانید هر یک از سرویس‌های دلخواه خود را انتخاب کنید. اما بسیاری از کاربران از ایمیل تحت وب به عنوان آدرس ایمیل اصلی خود استفاده می‌کنند. اگر شما این کار را می‌کنید، این نکته‌ی مهم را باید بدانید که سرویس‌های مختلف ارائه‌دهنده‌ی ایمیل، مزایا و معایبی دارند.

هات‌میل و یاهو مشکل امنیتی دارند و آن مشکل این است که آی‌پی رایانه‌ی فرستنده را به هر آدرس ایمیلی می‌فرستند. البته این ربطی به زمانی که شما به از طریق تُر ایمیل می‌فرستید، ندارد و آی‌پی تُر به جای آی‌پی شما به نمایش درمی‌آید. هر چند یاهو و هات‌میل درخواست پروتکل امنیتی HTTPS را نمی‌کنند- و مشکلی وجود ندارد تا تا زمانی که شما از تُر برای دسترسی به سرویس‌های ایمیل استفاده کنید. اما بسیاری از کاربران، ایمیل‌های خود را در مکان‌هایی چک می‌کنند که در آنجا تُر نصب نیست. برای حساب اصلی‌تان این مهم است که از سرویس‌دهنده‌ای استفاده کنید که پروتکل امنیتی HTTPS را ارائه می‌دهد.

Riseup.net سرویس‌دهنده‌ی ایمیل تحت وب با درجه‌ی امنیتی بسیار بالا است. آنها از سیستم کدگذاری PGP استفاده می‌کنند- و این زمانی بسیار مفید است که شما با افرادی در تماس باشید که آنها هم از PGP استفاده می‌کنند. شما می‌توانید به صورت رایگان در www.riseup.net حساب باز کنید و و از همکاران خود نیز بخواهید که در آنجا حساب باز کنند.

جی‌میل، تا زمانی که خودش را یک سرویس ایمیل امن معرفی نکرده بود، دارای نکات امنیتی خوبی بود. اگر شما به این آدرس بروید، (https://mail.google.com/mail)، تمام عملیات در جی‌میل به وسیله‌ی https کدگذاری می‌شود. همچنین می‌توانید به https://mail.google.com/h مراجعه کنید که ایمیل تحت وب جی‌میل براساس پروتکل امنیتی SSL است و طور خودکار به صورت HTML باز می‌شود. (من به شما پیشنهاد می‌کنم که این آدرس را ذخیره کنید و همواره از حساب جی‌میل خود از طریق این آدرس استفاده کنید). جی‌میل آی‌پی را در سربرگ ایمیل قرار نمی‌دهند و شما می‌توانید از سیستم کدگذاری PGP که جی‌میل آن را پشتیبانی می‌کند، استفاده کنید. برای این کار باید افزونه‌ی FireGPG را در فایرفاکس نصب کرده و بدینگونه امنیت در جی‌میل را افزایش دهید. FireGPG شما را در استفاده از صفحات وبی که از GnuPG استفاده می‌کنند، کمک می‌کند تا راحت‌تر با این صفحات کار کنید.

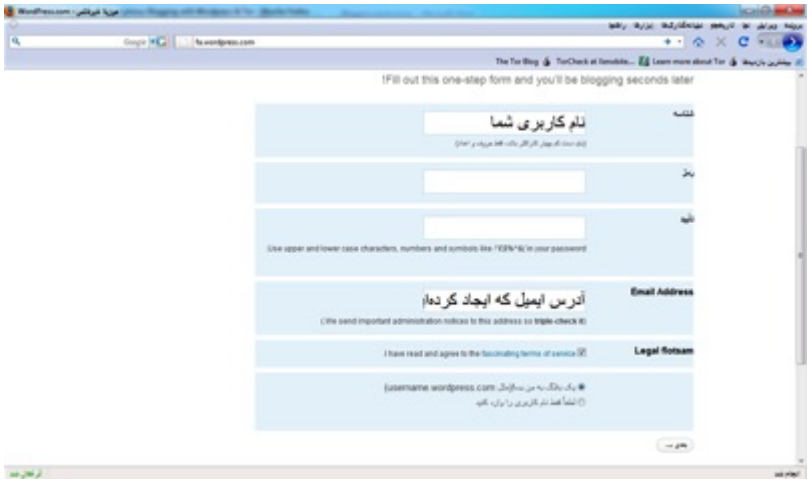


یک خطر که در تمام حساب‌های ایمیل تحت وب وجود دارد، اعتماد شما به شرکت ارائه‌دهنده‌ی ایمیل است که تمام ایمیل‌های شما را نگهداری می‌کند. اگر این شرکت مورد حملات خرابکارنه (هک) قرار بگیرد، یا توسط دولت‌ها برای انتشار اطلاعات، تحت فشار قرار بگیرد؛ آنها می‌توانند به متن تمام ایمیل‌هایی که شما دریافت کرده‌اید و یا فرستاده‌اید، دسترسی داشته باشند. تنها راه موجود نوشتن متن در ویرایشگرهایی است که متن‌ها را به صورت PGP کدگذاری می‌کنند و فرستادن آن به فرد دیگری است که وی نیز از PGP استفاده می‌کند. این بالاترین درجه‌ی امنیتی است که ما می‌خواهیم و به آن نیاز داریم، اما این مهم است که به خاطر داشته باشید که اعتماد به یک شرکت، ممکن است دردسرساز شود. به عنوان نمونه، یاهو،یک رفتار زننده در مورد دادن اطلاعات به دولت چین کرد (مخالفان چین هم اکنون این شرکت را به دلیل انتشار غیرقانونی اطلاعاتش تحت پیگرد قانونی قرار داده است). به همین دلیل کمی فکر کنید و سپس تصمیم بگیرید که به چه کسی می‌توان اعتماد کرد.

ب) تُر را بر روی مرورگر خود فعال کنید یا مرورگر تُر را از روی حافظه‌ی یواس‌بی خود اجرا کنید. به وب‌سایت سرویس ارائه‌دهنده‌ی ایمیل بروید و یک حساب جدید باز کنید. از هیچگونه اطلاعات شخصی‌تان استفاده نکنید. از نام کشورهایی مانند آمریکا یا بریتانیا استفاده کنید، که تعداد زیادی کاربر وب دارند. یک کلمه‌ی عبور مشکل برای حسابتان انتخاب کنید (دستکم هشت حرف باشد که شامل حداقل یک عدد یا یک علامت خاص باشد) و یک نام کاربری شبیه نام وبلاگی که می‌خواهید بنویسید، انتخاب کنید.

پ) مطمئن شوید که قادر به وارد شدن به سرویس ایمیل هستید و زمانی که تُر فعال است، می‌توانید ایمیل بفرستید. به دلیل اینکه تُر هر 10 دقیقه دچار تغییراتی در اتصال می‌شود، ممکن است که در عملیات ایمیل شما اختلال ایجاد کند، بنابراین باید این نکته را بدانید که برای نوشتن یک ایمیل جدید، تنها ده دقیقه وقت دارید و باید آن را در ده دقیقه انجام دهید.

الف) تُر را در مرورگر خود روشن کنید و یا بسته‌ی مرورگر تُر را فعال کنید. به Wordpress.com بروید و یک برای این کار کافی است که بر روی گزینه‌ی «همین حالا عضو شوید» کلیک کنید. از آدرس ایمیلی که قبلا ایجاد کرده‌اید، استفاده کرده و سپس نام کاربری که آدرس وبلاگ شما خواهد بود را انتخاب کنید: thenameyouchoose.wordpress.com

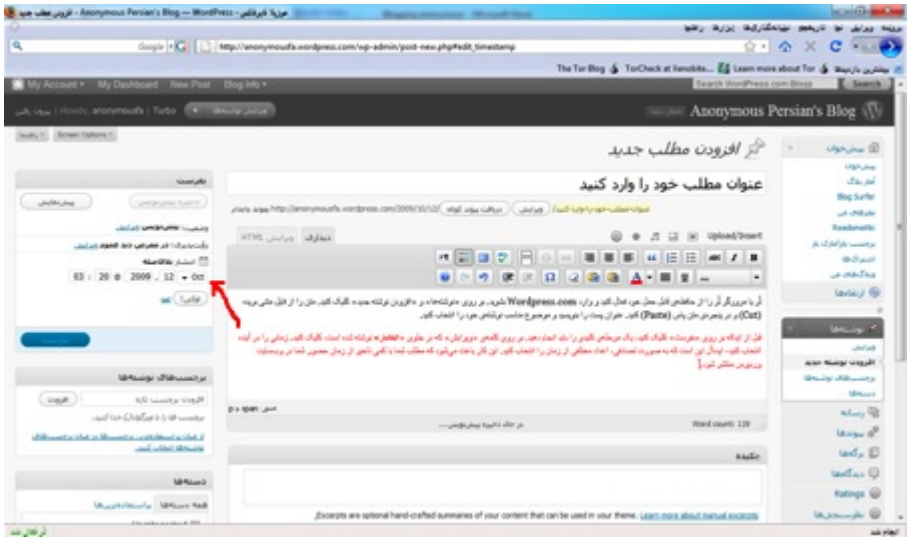


پ) وردپرس به آدرس ایمیل شما یک لینک برای فعال کردن حسابتان خواهد فرستاد. در حالی که تُر در مرورگر شما فعال است، ایمیل دریافت شده را باز کرده و بر روی لینک فعال‌سازی کلیک کنید. اینگونه وردپرس متوجه می‌شود که شما از یک آدرس ایمیل معتبر استفاده می‌کنید که آنها می‌توانند شما را از وضعیت بروزرسانی وب‌سایتشان، آگاه کنند. سرانجام آنها وبلاگ شما را به صورت عمومی نمایش می‌دهند و کلمه‌ی عبور را به ایمیل شما می‌فرستند. شما باید ایمیل خود را دوباره چک کنید تا کلمه‌ی عبور را به دست آورید.
پ) در حالی که از تُر استفاده می‌کنید، با نام کاربری و کلمه‌ی عبور، به وبلاگ جدیدی که ایجاد کرده‌اید، وارد شوید. بر روی «پیش‌خوان» کلیک کنید و سپس از روی ستون سمت راست، بر روی «کاربران» و «شناسه‌نامه شما» کلیک کنید. به قسمت «**رمز جدید**» بروید و در آنجا یک کلمه‌ی عبور مشکل وارد کنید که بتوانید آن را به خاطر بسپارید. در مورد بقیه‌ی اطلاع هم به خودتان بستگی دارد که علاقه دارید آنها را تکمیل کنید یا نه. اما این نکته را فراموش نکنید که اطلاعات وارد شده، ربطی به شما نداشته باشند.

مرحله چهارم: نوشتن در وبلاگ

این روش نه تنها یک راه حل خوب برای جلوگیری از، از بین رفتن یک پست بر اثر خرابی (crash) مرورگر یا قطع ارتباط اینترنتی است، بلکه روشی است برای آنکه شما مطالب خود را در هر جایی به صورت خصوصی‌تر از کافی‌نت بنویسید. یک ویرایشگر ساده مانند Wordpad در ویندوز، بهترین انتخاب برای استفاده است. مطالب خود را به صورت فایل‌های متنی ذخیره کنید (بعد از وبلاگ‌نویسی، همیشه یادتان باشد که فایل‌ها را به صورت کامل از روی رایانه‌ی خود حذف کنید، برای این کار از ابزارهایی مانند Eraser یا Ccleander که به چندین زبان در دسترس هستند و فایل‌های موقتی را که مرورگرها و برنامه‌های دیگر به صورت خودکار آن‌ها را ایجاد می‌کنند، حذف می‌کند.)

پ) تُر یا مرورگر تُر را از حافظه‌ی قابل حمل خود فعال کنید و وارد Wordpress.com بشوید. بر روی «نوشته‌ها» و «افزودن نوشته جدید» کلیک کنید. متن را از فایل متنی بریده (Cut) و در پنجره‌ی متن پاس (Paste) کنید. عنوان پست را بنویسید و موضوع مناسب نوشته‌ی خود را انتخاب کنید.
پ) قبل از اینکه بر روی «بفرست» کلیک کنید، یک مرحله‌ی کلیدی را باید انجام دهید. بر روی کلمه‌ی «ویرایش» که در جلوی «**انتشار**» نوشته شده است، کلیک کنید. زمانی را در آینده انتخاب کنید- ایده‌آل این است که به صورت تصادفی، اعداد مختلفی از زمان را انتخاب کنید. این کار باعث می‌شود که مطلب شما با کمی تاخیر از زمان حضور شما در وب‌سایت وردپرس منتشر شود.



چرا؟

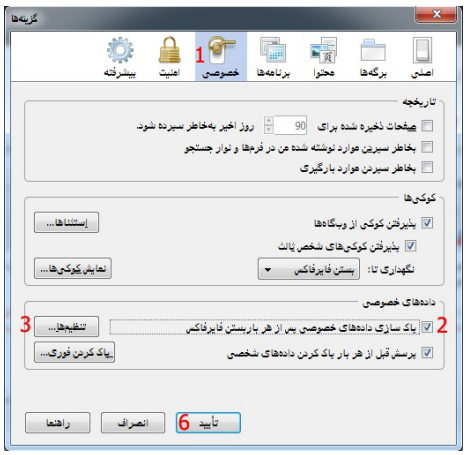
به وسیله‌ی ویرایش زمان انتشار، ما شما را در مقابل روشی که برخی از افراد برای شناسایی از آن استفاده می‌کنند، محافظت می‌کنیم. فرض کنید که شما وبلاگی می‌نویسید که نامش «مرگ بر شرکت مخابرات اتیوپی!» است. یک نفر در این شرکت ممکن است شروع به دنبال کردن این وبلاگ بکند و متوجه شود که یکی از مشتریانش این وبلاگ را می‌نویسد. آنها شروع می‌کنند به بررسی زمان‌هایی که مطالب از طریق وردپرس دات کام منتشر شده است و سپس آن را با اطلاعاتشان مقایسه می‌کنند. آنها کشف می‌کنند که در یک دوره‌ی زمانی خاص این پست‌ها نوشته می‌شود و در نهایت متوجه می‌شود که مشتریانشان از یک یا دو سرور تُر استفاده می‌کنند. در نهایت می‌فهمند که کاربر از تُر برای فرستادن پست‌هایش استفاده می‌کند و براساس همین اطلاعات، به پلیس گزارش می‌دهند.

یا تغییر زمان انتشار پست‌ها، ما این روش برخورد سروبس دهندگان اینترنت را سخت‌تر می‌کنیم. هم اکنون آنها نیاز به دسترسی به اطلاعات ثبت شده در سرورهای وردپرس دارند که دسترسی به آنها بسیار سخت است. این یک روش ساده است که امنیت شما را افزایش می‌دهد.

قدم پنجم: پوشاندن ردپاهایتان

الف) پاک کردن پیش‌نویس‌های مطالب‌تان از روی لپ‌تاپ یا رایانه‌یتان باید با امنیت کامل انجام شود. اگر شما از حافظه‌های یواس‌بی برای منتقل کردن پست‌هایتان به کافی‌نت استفاده می‌کنید، شما باید آنها را هم پاک کنید. تنها جابه‌جا کردن فایل‌ها به سطل زباله و خالی کردن آن کافی نیست- شما به ابزارهای پاک کردن امنی مانند Earser یا Ccleaner که تمام فایل‌ها و اطلاعات قدیمی را که ممکن است زمانی بازیابی شود را پاک می‌کنند، نیاز دارید. بر روی مکینتاش، این ابزار وجود دارد و زمانی که شما فایلی را به صندوق زباله بیندازید، با انتخاب گزینه‌ی «Secure Empty Trash» این کار را می‌توانید انجام دهید.

ب) تاریخچه، کوکی‌ها و پسوردها را از فایرفاکس پاک کنید. از منوی ابزارها، گزینه‌ی «پاکسازی اطلاعات خصوصی» را انتخاب کنید. تمام گزینه‌ها را چک بزنید و بر روی «پاکسازی فوری اطلاعات خصوصی» کلیک کنید. ممکن است شما بخواهید زمانی که از فایرفاکس خارج می‌شود، فایرفاکس به صوت خودکار تمام اطلاعات را پاک کند. شما می‌توانید برای این کار این مسیر را طی کنید: «فایرفاکس< ابزارها< گزینه‌ها< خصوصی< تنظیم‌ها» و گزینه‌ی «پاک‌سازی داده‌های خصوصی پس از هر بار بستن فایرفاکس» را چک بزنید. در حالتی که شما نمی‌توانید برنامه‌ای را بر روی رایانه نصب کنید، از ابزار IE Privacy Cleaner که می‌توانید آن را به کمک حافظه‌ی یواس‌بی خود حمل کنید، استفاده کنید.



چرا؟

برای یک نفر این بسیار ساده است که از طریق بررسی تاریخچه‌ی مرورگر شما، بفهمد که شما از چه وب‌سایت‌هایی بازدید کرده‌اید. افراد حرفه‌ای می‌توانند از طریق چک کردن فایل‌های کچ (Cach) که چندین نسخه از صفحات وب را ذخیره می‌کند، تاریخچه‌ی مرورگر شما را پیدا کنند. ما می‌خواهیم تمام این اطلاعات از رایانه‌های عمومی پاک شوند که کاربران دیگر نتوانند آنها را بدست بیاورند. و ما می‌خواهیم تمامی این اطلاعات از رایانه‌های شخصی هم پاک شود، چون اگر حادثه‌ای مانند دزدی، گم شدن و ضبط شدن رخ بدهد، آنها از مطالبی که ما نوشته‌ایم باخبر می‌شوند.

برخی نکات حاشیه‌ای:

- این تنها کافی نیست که در زمان نوشتن از خودتان محافظت کنید. اگر شما قصد دارید که در وبلاگ دیگران نظری بدهید، باید باز هم از تُر استفاده کنید. اکثر نرم‌افزارهایی که وبلاگ‌ها با آنها مدیریت می‌شوند، آی‌پی نظردهنده را نشان می‌دهند. اگر شما از تُر استفاده نکنید، شما دیگران را دعوت کرده‌اید که آی‌پی رایانه‌ی شما را ردیابی کنند. تُر مانند کاندوم است! به صورت ناامن تمرین وبلاگ‌نویسی نکنید.
- چون شما ناشناس هستید، نباید وبلاگ شما چهره‌ای نازیبا داشته باشد. از گزینه‌ی «نما» در وردپرس چندین گزینه دارید که می‌توانید وبلاگتان را زیبا کنید. شما می‌توانید از پوسته‌های مختلف استفاده کنید، یا برای سفارشی کردن برخی از آنها عکس آپلود کنید. اما بسیار بسیار مراقب تصاویر خودتان، باشید. شما با انتشار یک تصویر، اطلاعات زیادی در مورد خودتان می‌دهید (برای مثال، اگر یک عکس در زیمباوه گرفته شده باشد، این ثابت می‌کند که شما در زیمباوه هستید یا بوده‌اید.)
- اگر شما واقعا نگران امنیت خود هستید، می‌توانید یک قدم بیشتر بردارید و در تنظیمات مرورگر فایرفاکس، جاوا را غیرفعال کنید. چند حفره‌ی امنیتی در نسخه‌های اخیری که از جاوا منتشر شده است وجود دارد که به اسکریپت‌های خرابکار اجازه می‌دهد تا آی‌پی رایانه‌ی شما را شناسایی کنند، **هر چند شما از تُر استفاده بکنید.** ما زیاد نگران این مورد نیستیم، زیرا فکر نمی‌کنیم که وردپرس دات کام یا گوگل این اسکریپت‌های خرابکار را اجرا می‌کنند... اما در برخی زمان‌ها، این مورد بسیار جدی است. برای غیر فعال کردن جاوا این مسیر را طی کنید: «فایرفاکس< ابزارها< گزینه‌ها< محتوا» و چک گزینه‌ی «فعال بودن جاوا» را بردارید.

- اگر شما تنها فردی باشید که در کشورتان از تُر استفاده می‌کنید، این بسیار واضح است! یک کاربر، تنها کسی است که از آی‌پی یکی از شبکه‌های تُر استفاده می‌کند. اگر شما از تُر استفاده می‌کنید و از این نگران هستید که سرویس ارائه‌دهنده‌ی خدمات اینترنتی (ISP) ممکن است در مورد استفاده‌کنندگان تُر تحقیقات بکند، شما می‌توانید دیگر

دوستانتان را به استفاده از تُر تشویق کنید، که در اصطلاح به آن ترافیک پوششی (Cover Traffic) می‌گویند.
همچنین شما ممکن است که تنها برای نوشتن وبلاگ از تُر استفاده نکنید و بخواهید از تُر برای خواندن وب‌سایت‌های مختلف استفاده کنید. در هر دو مورد، این بدان معنا است که تُر برای دلایلی دیگر غیر از نوشتن وبلاگ به صورت ناشناس استفاده می‌شود، یعنی کاربر با دسترسی به تُر نمی‌تواند به صورت خودکار سرویس ارائه‌دهنده‌ی خدمات اینترنتی (ISP) را به اشتباه بیاندازد.
و آخرین ایده در مورد گمنامی: اگر شما واقعا نیازی ندارید، ناشناس نباشید و اگر اسم شما با مطالبتان همراه باشد، مردم سخنان شما را جدی‌تر می‌گیرند. اما برخی مردم احتیاج دارند که ناشناس بمانند و این دلیل وجود همین راهنما است. پس تا زمانی که نیاز ندارید، از این تکنیک‌های استفاده نکنید.

حمایت از ما را فراموش نکنید!