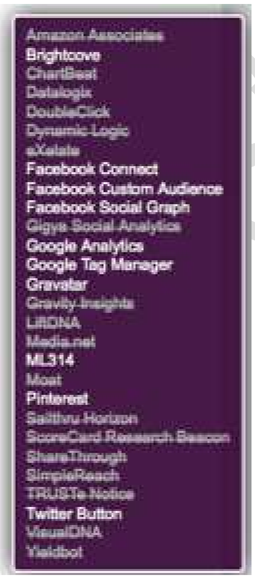
# Welcome to Securing Your Digital Footprint

## Browsers-

Taking online security steps is not an act of paranoia. Online security is something we have all been lackadaisical about for too long. Considering the political climate we now live in, it is time to take this next step in protecting your online presence. In this article, I'm focusing on browsers.

Browsers are programs which allow us to access the internet; you know them as Firefox, Internet Explorer, Safari and others. Advertisers place files, called cookies, on your browser to keep track of the pages you visit online.

Below is a list of companies tracking me as I accessed a website today.



~~Amazon Associates~~
Brightcove
~~ChartBeat~~
~~Datalogix~~
~~DoubleClick~~
~~Dynamic Logic~~
~~eXelate~~
Facebook Connect
Facebook Custom Audience
Facebook Social Graph
~~Gigya Social Analytics~~
Google Analytics
Google Tag Manager
Gravatar
~~Gravity Insights~~
~~LiRDNA~~
~~Media.net~~
ML314
~~Moat~~
Pinterest
~~Sailthru Horizon~~
~~ScoreCard Research Beacon~~
~~ShareThrough~~
~~SimpleReach~~
~~TRUSTe Notice~~
Twitter Button
~~VisualDNA~~
~~Yieldbot~~

These entities record every search I make, each website I access, how long I spend there, and what I do there; you get the picture. What do they do with all the information they collect? I don't know about you, but I don't like being tracked.

So how do you increase your online security by way of browsers?

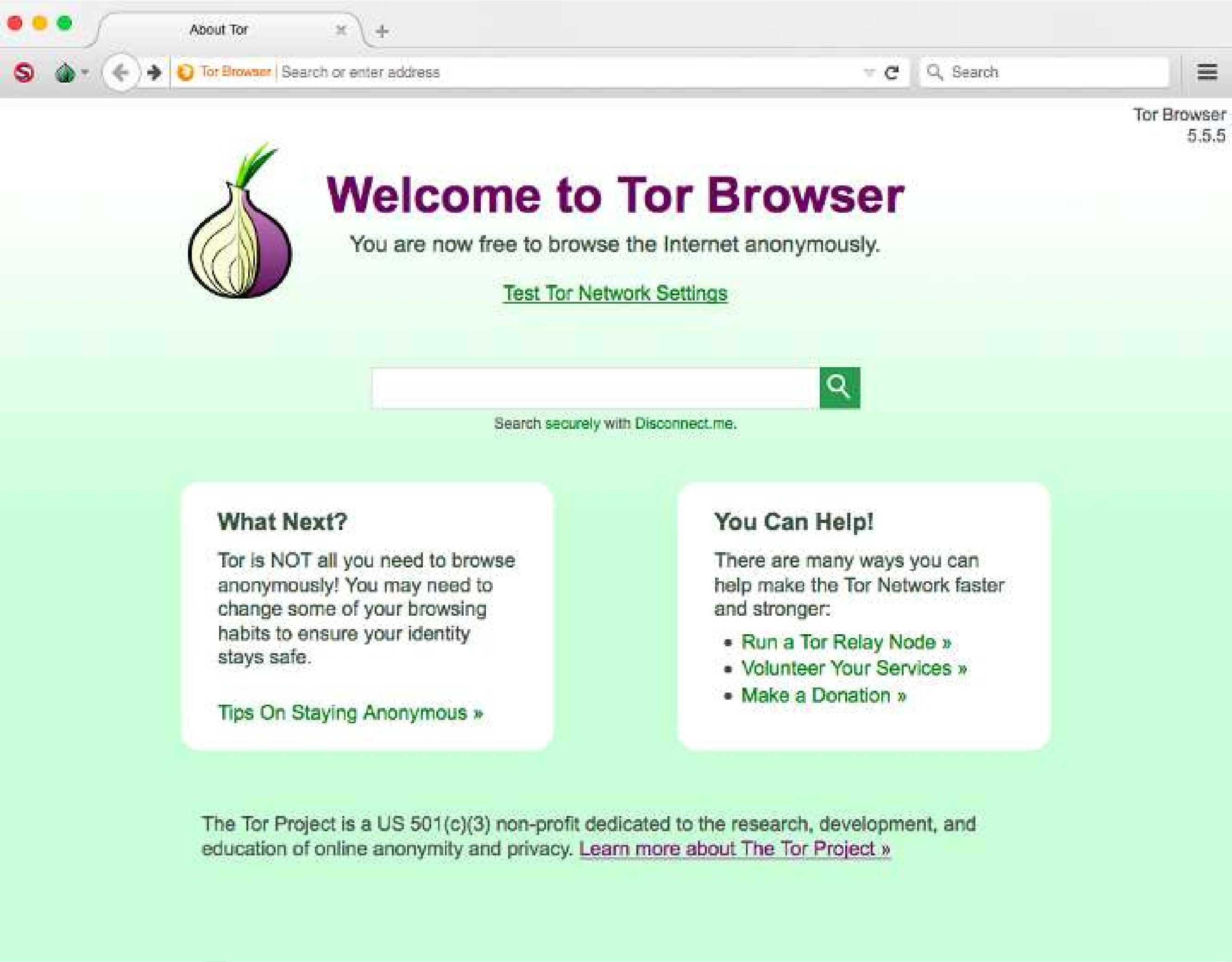
First, if you are using Internet Explorer – STOP. It is, by far, the worst program ever released on an unsuspecting population. More security holes have been reported by this program than any other.

Second, install an "add on" program like Ghostery or Privacy Badger to identify trackers, and stopping them from getting *your* info.

Third, when you connect to the Web, some sites offer both unsecured (HTTP) and secured (HTTPS) versions of the web page; to automatically connect to the secured versions of available websites, install HTTP Everywhere.

Fourth, the cookies placed on websites to track our interests and then advertisers customize ads and deliver them to your inbox. These ads can contain malware. Installing uBlock Origin will block potentially malicious content. Also scan your computer for malware once a week using Malwarebytes.

Fifth, stop using Google, Bing, Yahoo or whatever other search engine you are using. Start using DuckDuckGo - simply type it into the URL, set it as your default search engine. They never track you.
Sixth, stop using Firefox, Chrome, Safari, etc., as your browser. Brave or Epic don’t track you.
When you close and open most browsers they will allow you to do a ‘restore last’ to re-open all of the previous tabs. This is a security hole which Epic will not allow. Which ever browser you choose make sure you turn off javascript.
To be truly secure you need to download and only use Tor; it's the most secure of all the browsers.



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

- The Tor browser encrypts your traffic and bounces your secured connection within the Tor network
- before connecting to the Web from a remote location. For example, if you connect to a website (e.g.,
- duckduckgo.com) within the Tor browser, it may appear to connect from a different country. Connecting

- through Tor can be a little slower than a standard browser, but it’s helpful for sharing information
- anonymously, avoiding surveillance, or accessing censored web pages. It is important to note that network
- eavesdroppers can still tell that you’re using Tor, they just can’t tell what you’re doing within it. Tor will not
- allow you to save your opened tabs for a restore “previous session.”
- The other nice thing about Tor is it can be set it up so that everything on your computer will go through it giving your computer even more security.
-
- 1. Open the Tor browser
- 2. Click on the hamburger menu (3 lines stacked - right hand corner of browser window)
- 3. Click Preferences
- 4. Click Advanced
- 5. Click Network
- 6. Under ‘Connection’ Click Settings
- 7. In the window that pops up, under ‘Manual Proxy Settings’ see ‘Socks’
- 8. Copy the numbers under ’Socks’
- 9. Open the Network settings for your computer
- 10. The numbers you got from Tor will need to be entered under ‘Socks’ for proxies
- Once you have accomplished this, your computer will be using Tor for everything related to internet traffic.

Since I wrote this article, last week, new information is out about Tor: stating that it is a known ‘haven,’ if you will for people looking to evade the state or do something nefarious. Source: Also it is based on the Firefox browser, which is on a rigid schedule for bug fixes, making it less secure. Bottom line, might be better if you use Brave, DuckDuckGo and a VPN.

UPDATE: We’ve been using Tor for several weeks, both as a browser and as mock VPN. As a browser it is slow, reminiscent of the days of dial up, occasionally you will be blocked from accessing websites. As a VPN - run all Internet traffic through it - one day none of our email accounts could be accessed.

While we’re on the subject, let’s take a moment and talk about browser history.

Congress decided in April 2017 to allow ISP’s (Verizon, AT&T, Comcast, etc.) to sell our browsing history. This is huge blow to privacy. You may be asking what exactly is ‘browser history?’ Any time you open up a search engine (Google, Yahoo, Bing, Safari, etc.) and type something in. Like an embarrassing medical condition you’ve been doing Google searches on? Or that little surprise gift you’re getting for your spouse, to make your marriage burn brighter? Maybe you overheard a conversation at the grocery store/water cooler and decided to do a search to find out what they were talking about. How were you supposed to know it was a new form of sex bondage? All of that and so much more makes up our browser histories.

We shouldn’t really be surprised that these companies are salivating to make money off our privacy. After all Facebook and Google have been doing it for years.

To be safe, interacting with the Internet we need to take some steps. Stop using Google as your search engine. They know too much as it is. Follow the instructions in this story to find out what Google knows about you and to delete that information.

Your new search engine should be DuckDuckGo, they don’t track you, nor do they keep any of your search results. Their search results are just as extensive as Google.

Next, use Brave as your browser. Unlike Firefox, Safari, Chrome, etc., they don’t track you. It’s more secure if you don’t save and reopen tabs when you open your browser. (Not a paid spokesperson for either of these companies)

Both of these options are available for Apple, Windows, iPhones and Androids. On the iPhone you will have to go into Settings and turn off ‘Cellular Data/Wifi’ for Safari. As it is the default browser and can’t be deleted.

Being smarter about digital/online/technology security should be a part of everyday life, now that we are so dependent on our devices.

If you take these security steps, you are taking an excellent step toward protecting your online presence.  Please see my next article on cellphones, iPads, tablets for more security suggestions.