Practical Paranoia™ macOS 10.13

Security Essentials

☑ The Easiest

☑ Step-By-Step

☑ Most Comprehensive

☑ Guide To Securing Data and Communications

☑ On Your Home and Office macOS Computer

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Notice of Liability: The information in this document is presented on an *As Is* basis, without warranty. While every precaution has been taken in the preparation of this document, the author shall have no liability to any person or entity with respect to any loss or damage caused by or alleged to be caused directly or indirectly by the instructions contained in this document, or by the software and hardware products described within it. It is provided with the understanding that no professional relationship exists, and no professional security or Information Technology services have been offered between the author or the publisher and the reader. If security or Information Technology expert assistance is required, the services of a professional person should be sought.

Trademarks: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the author was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified in this document are used in editorial fashion only and for the benefit of such companies with no intention of infringement of trademark. No such use, or the use of the trade name, is intended to convey endorsement or other affiliation within this document.

Editions: v1.0 20170918 • v1.01 20170923 • v1.1 20171001 • v1.2 20171022 • v1.3 20180325 • v2 20180420

Cover design by Ed Brandt

ISBN-10: 1976513650
ISBN-13: 978-1976513657

Dedication

To Candace,
without whose support and encouragement
this work would not be possible

Contents At A Glance

Contents In Detail

14 Web Browsing

Distrust and caution are the parents of security.

–Benjamin Franklin[1]

What You Will Learn In This Chapter

- Install HTTPS Everywhere
- Choose a browser
- Enable private browsing
- Enable secure web searches
- Clear browser history
- Install browser plug-ins
- Find and remove browser extensions
- Detect fraudulent websites
- Issues with Adobe Flash and Java
- Recover from a web scam
- Install Tor for anonymous browsing
- Find if you’ve been pwned

[1] *https://en.wikipedia.org/wiki/Benjamin_Franklin*

14.1 HTTPS

Due to an extraordinary marketing campaign, everyone knows the catchphrase: *What happens in Vegas, stays in Vegas*. With few exceptions, web surfers think the same thing about their visits.

Most websites use HTTP[2] (Hypertext Transport Protocol) to relay information and requests between user and website and back again. HTTP sends all data in clear text–anyone snooping on your network connection anywhere between your computer and the web server can easily see everything that you are doing.

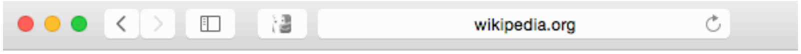
Typically, the only exceptions you will come across are financial and medical sites, as they are mandated by law to use HTTPS[3] (Hypertext Transport Protocol Secure). HTTPS uses the SSL[4] (Secure Socket Layer) encryption protocol to ensure that all traffic between the user and server is military-grade encrypted.

- Note: With the recent changes in Google Search Engine Optimization[5] (SEO) guidelines that give a higher priority to HTTPS sites, it will soon become common for sites to use encryption.

Although it is unlikely that you would ever be in the position to enter your password or bank account into an unsecure web page, you are almost guaranteed to enter your identity information, such as full name, address, phone number, and social security number. It is effortless for an identity thief to copy this information.

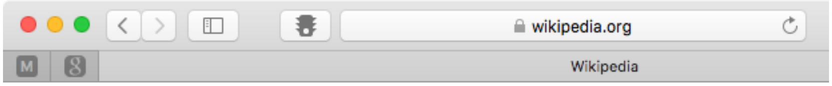
Anytime that you visit a web page that is secured using https, it will be reflected in the URL or address field of your web browser.

In the following example, I visit Wikipedia.org by entering *http://www.wikipedia.org* in my browser address field:



[2] *https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol*
[3] *https://en.wikipedia.org/wiki/HTTPS*
[4] *https://en.wikipedia.org/wiki/Transport_Layer_Security*
[5] *https://en.wikipedia.org/wiki/Search_engine_optimization*

In the next example, I visit Wikipedia again, but this time I enter *https://www.wikipedia.org* in the address field:



Note how the address field reflects that I am now connected securely by displaying https and the *Lock* icon. Each browser will indicate security slightly differently–some displaying just the https, some just the lock.

- Note: As of this writing, Wikipedia has implemented automatic forwarding from HTTP to HTTPS, so if you enter *http://wikipedia.org*, you are automatically forwarded to *https://wikipedia.org.*

Now that I am connected securely to Wikipedia, snoops will not be able to see my actions. However, they still can see that I am connected to Wikipedia. If you would like to shield yourself completely, continue reading to our chapter on using a Virtual Private Network (VPN.)

Having to remember to connect via HTTPS for each web page is an impossible task. First, you have other, more important items to store in your synapses. Second, many websites do not have an HTTPS option, resulting in many error pages and wasted time during the day.

There are two options to resolve this:

- Automate the attempt to connect to sites via HTTPS
- Encrypt your entire online session using VPN

Using VPN is covered in a later chapter. Automating the attempt to connect via HTTPS is both easy and free. All it requires is a freeware plug-in, *HTTPS Everywhere.*

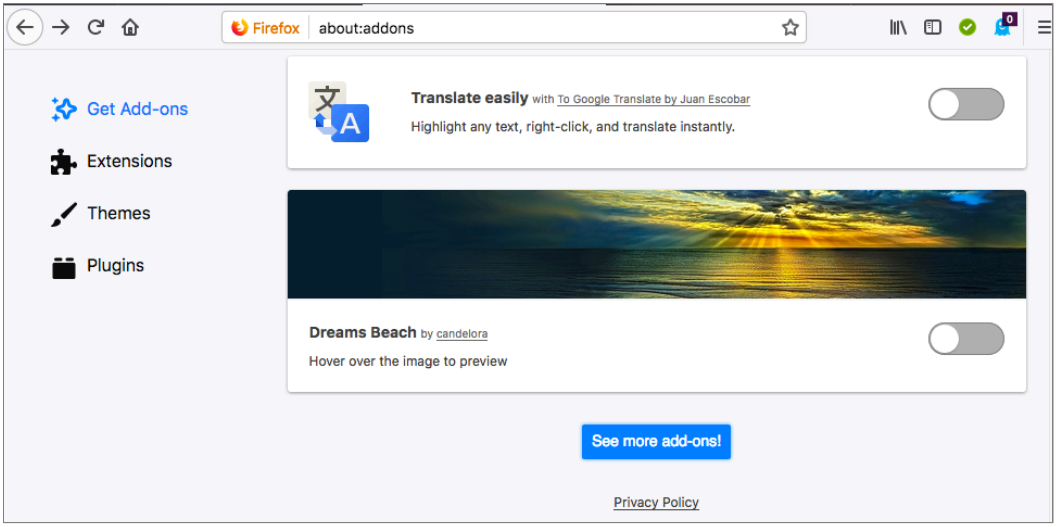
HTTPS Everywhere is available for Firefox, Opera, and Chrome. Unfortunately, this currently leaves Safari users without the option. If you are happy to use either of these two browsers instead of Safari, there is no reason not to install HTTPS Everywhere!

14.1.1 Assignment: Install HTTPS Everywhere

HTTPS Everywhere is available for Firefox, Opera, and Chrome.

In this assignment, you install HTTPS Everywhere into Firefox.

1. If the Firefox browser is not currently installed, open Safari, and the go to *http://firefox.com* to download Firefox.
2. Open Firefox.
3. Select the *Tools* menu > *Add-ons.*
4. Select *Get Add-ons* from the sidebar, scroll to the bottom of the page, and then select the *See more add-ons!* button.

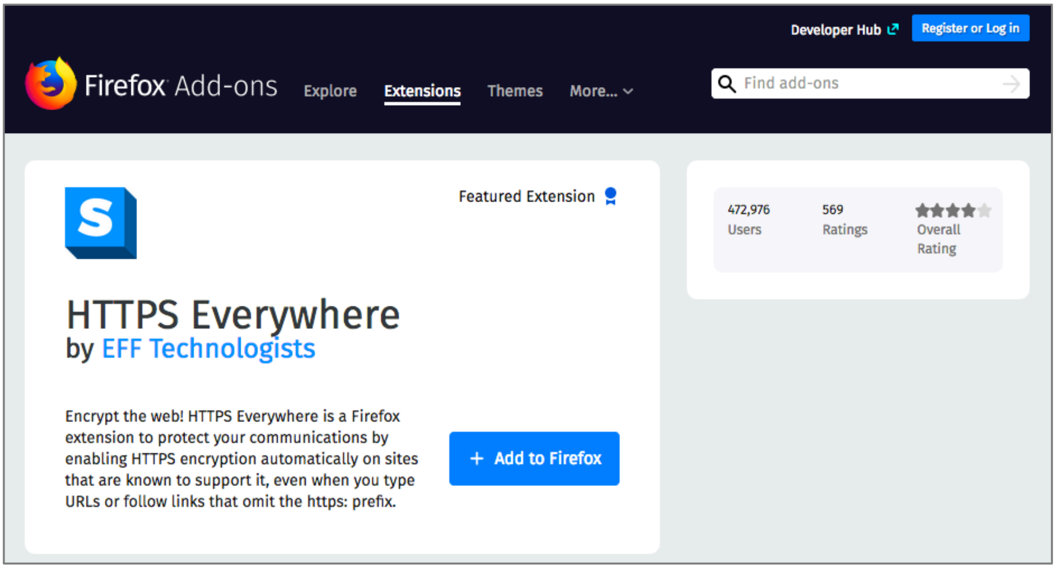


about:addons

Translate easily with To Google Translate by Juan Escobar
Highlight any text, right-click, and translate instantly.

Dreams Beach by candelora
Hover over the image to preview

5. In the *Search* field, enter *https everywhere,* and then press the *Return* key. Matching items will appear below.



HTTPS Everywhere
by EFF Technologists

Encrypt the web! HTTPS Everywhere is a Firefox extension to protect your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type URLs or follow links that omit the https: prefix.

6. Select the *Add to Firefox*. HTTPS Everywhere will download.
7. At the *Add HTTPS Everywhere?* confirmation window, select the *Add* button, and then the *OK* button.
8. HTTPS Everywhere is now installed in Firefox.

You can repeat this process for Chrome and Opera.

14.2 Choose a Browser

There many web browsers available on the market, with each placing a different emphasis on various features. The most popular browsers for macOS are Safari, Mozilla Firefox, and Google Chrome. Safari is included with macOS, while Chrome and Firefox are available as free downloads. Why might you want to replace Safari with another browser? Chrome integrates tightly with Google's own services, offering features such as direct voice translation and an ultra-minimalistic interface. Firefox touts itself as the most privacy-respecting browsers, and while that is a subjective claim, Firefox does not transmit your data to Google or any other 3rd party company every time you search using the address bar box. While Google considers this "non-identifying information", IP addresses are identifying at the Internet Service Provider level. This functionality can be changed, and with some tweaking, it is possible to make Chrome more privacy focused.

Browser	**Platform**	**Price**	**Notable Features**	**Privacy**
Chrome	Android, iOS, Linux, macOS, Windows	Free	Speed Google Services Integration History and Bookmarks can be shared between your devices running Chrome	Fair
Edge	Windows 10	Free (included with Windows 10)	Active X Windows Integration	Fair
Firefox	Android, iOS, Linux, macOS, Windows	Free (Open Source)	Add-ons Privacy History and Bookmarks can be shared between your devices running Firefox	Good

Safari	macOS, iOS	Free (included with macOS/OS X and iOS)	History and Bookmarks can be shared between all your macOS and iOS devices	Good

14.3 Private Browsing

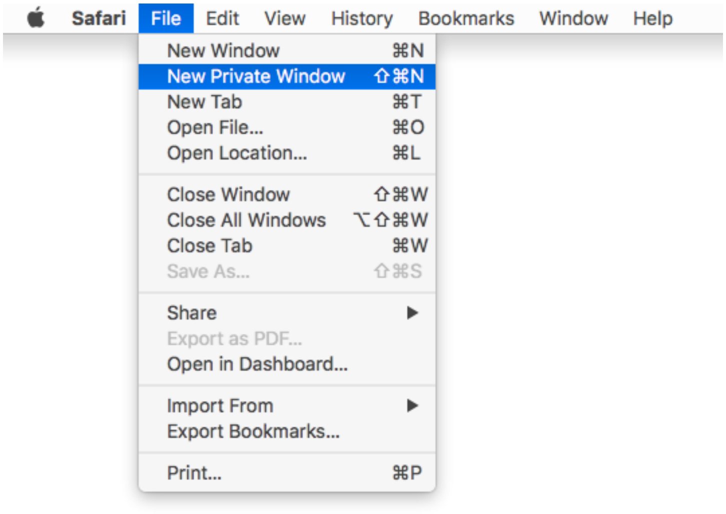
Private Mode (Safari), *Private Browsing* (Firefox), and *Incognito Mode* (Chrome), are features that prevent any normally cached data from being written to storage while using a browser. This data includes browsing history, passwords, user names, list of downloads, cookies, and cached files. This is an essential tool if you work on a computer where your account is shared (what's with that?.), or if there is the possibility that someone else will examine your browsing habits. This does not prevent your company IT department or Internet Provider from seeing or recording your browsing habits.

14.3.1 Assignment: Safari Private Browsing

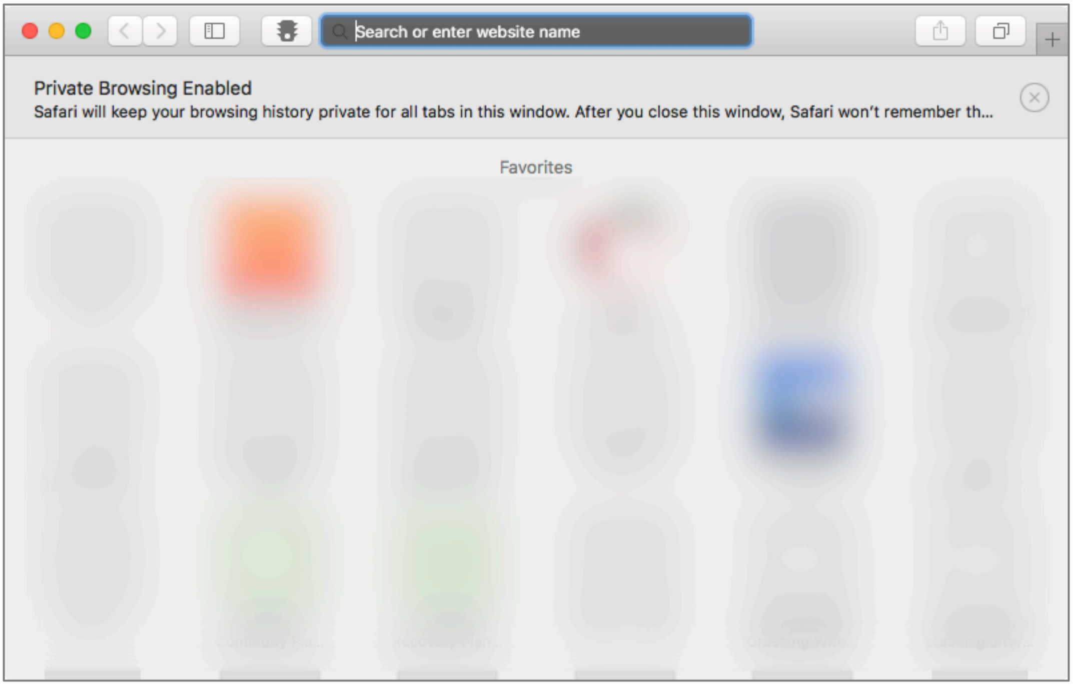
Before we secure your website travels from roaming eyes out on the Internet, we should first be secure from the roaming eyes on the home front. If you have secured your computer to this point, including: Strong password, nobody else has access to your account, your *System Preferences > Security & Privacy* are set to *Require password after sleep or screen saver begins*, it is unlikely that you also need to implement *Safari Private Browsing*. But just in case…

In this assignment, you enable Private Browsing within Safari

1. From the *Safari File* menu, select *New Private Window*.



2. A new Safari window will appear. You can see that you are in *Private Browsing* by the *Search* field being dark.



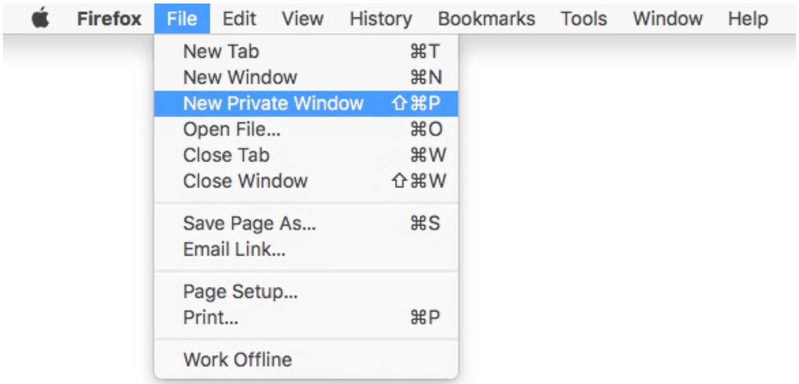
Private Browsing Enabled
Safari will keep your browsing history private for all tabs in this window. After you close this window, Safari won't remember th...

Sites that are visited from within this window will leave no trace in the *History*, and cookies are not shared with any other browsing windows.

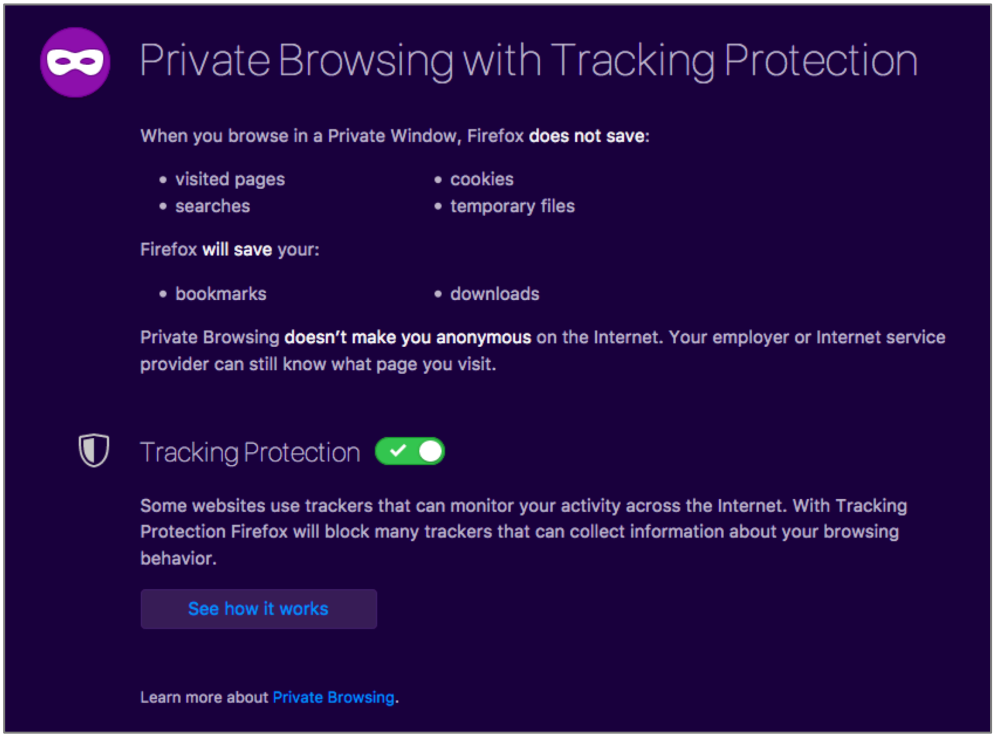
14.3.2 Assignment: Firefox Private Browsing

If you prefer Firefox to Safari, then let us enable its private browsing.

1. Launch Firefox.
2. Select the Firefox *File* menu > *New Private Window*.



3. A new *Private Window* opens, informing that you are now, well, browsing privately.
   - Note: A Firefox *Private Window* will display a mask icon in the left side of a private tab, and in the top right corner of a private window.



Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- searches
- cookies
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.

Tracking Protection ✓

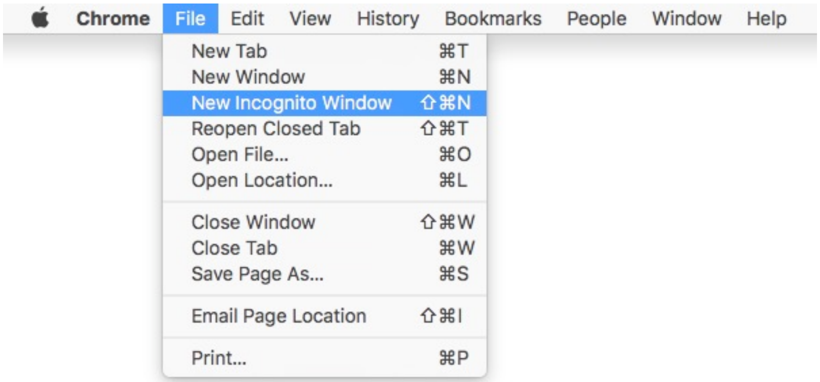
Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

Learn more about Private Browsing.

14.3.3 Assignment: Google Chrome Incognito Mode

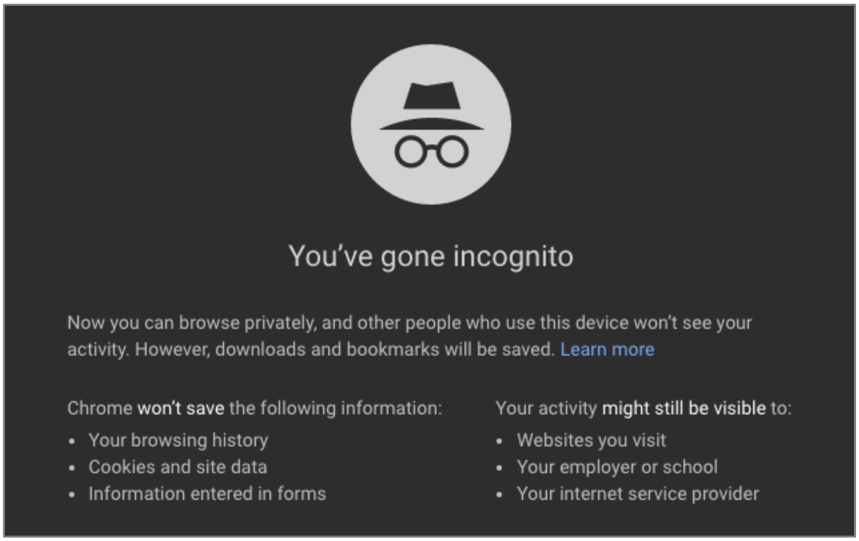
If your preference leans toward Google Chrome, you can enable its *Incognito Mode*.

1. Launch Google Chrome.
2. Select the *File* menu > *New Incognito Window*.



3. A new *Incognito Window* opens, informing that you have now, gone incognito.

    - Note: A Chrome *Incognito Window* will display the incognito icon in the top right corner, and the title bar will turn dark.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

14.4 Secure Web Searches

With most web browsers, when performing a search, the search criteria and sites visited are collected and stored by the search engine. The Cookies assigned from one website can communicate with other sites and webpages you open. Also, most search engines record your searches and build a profile of your search history so that your search results will be unique and tailored to your interests.

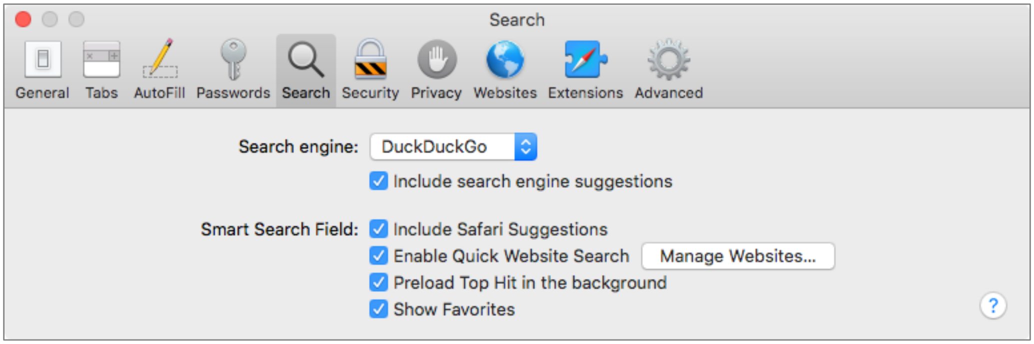
Not so with the *DuckDuckGo* search engine. DuckDuckGo's policy is that it keeps no information on user searches, nor does it track search queries via IP addresses. Subsequently, all search results are identical for everyone.

Starting with OS X 10.10, Safari offers the option to make DuckDuckGo your default search engine. This is a big step towards providing a better level of privacy on the Web.

14.4.1 Assignment: Make DuckDuckGo Your Safari Search Engine

In this assignment, you change the default Safari search engine from Google to the secure search engine DuckDuckGo.

1. Open Safari.
2. Open the *Safari* menu > *Preferences*.
3. Select the *Search* icon from the Toolbar.
4. From the *Search Engine* pop-up menu, select *DuckDuckGo*.



Search engine: DuckDuckGo
☑ Include search engine suggestions

Smart Search Field: ☑ Include Safari Suggestions
☑ Enable Quick Website Search
☑ Preload Top Hit in the background
☑ Show Favorites

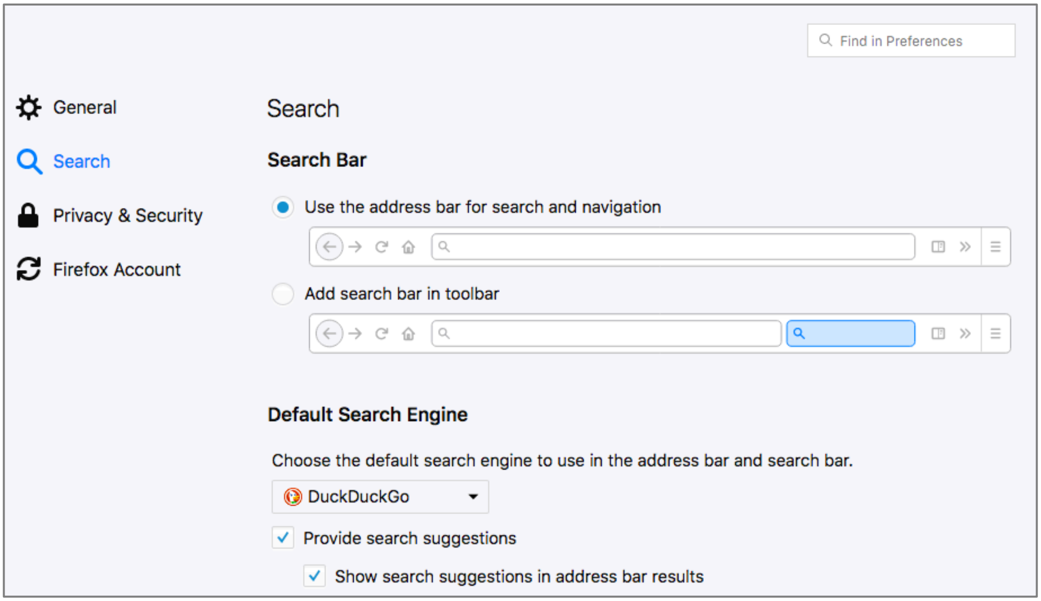
5. Close the Preferences window.

From now on, your default search engine for Safari will be *DuckDuckGo*, hiding your search activities.

14.4.2 Assignment: Make DuckDuckGo Your Firefox Search Engine

In this assignment, you change the default Firefox search engine to the secure DuckDuckGo.

1. Open Firefox.
2. Select the *Firefox* menu > *Preferences*.
3. Select *Search* from the sidebar, and then select *DuckDuckGo* from the *Default Search Engine* pop-up menu.



Search

Search Bar

● Use the address bar for search and navigation

○ Add search bar in toolbar

Default Search Engine

Choose the default search engine to use in the address bar and search bar.

DuckDuckGo

☑ Provide search suggestions

☑ Show search suggestions in address bar results

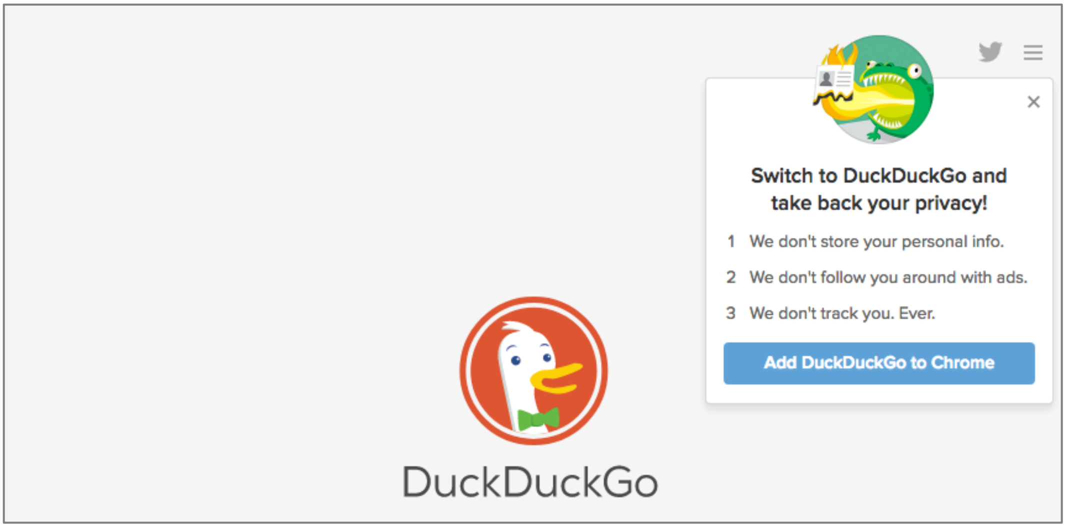
4. Close the Preferences window.

From now on, your default search engine for Firefox will be *DuckDuckGo*, hiding your search activities.

14.4.3 Assignment: Make DuckDuckGo Your Chrome Search Engine

In this assignment, you change the default Chrome search engine to DuckDuckGo.

1. Open Chrome.
2. Go to *https://duckduckgo.com.*
3. On the DuckDuckGo home page, select *Add DuckDuckGo to Chrome.*



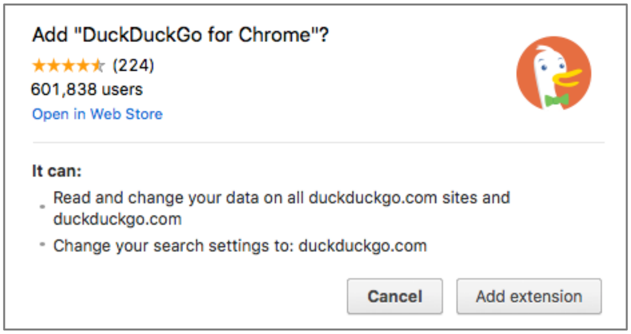
Switch to DuckDuckGo and take back your privacy!

1 We don't store your personal info.

2 We don't follow you around with ads.

3 We don't track you. Ever.

4. At the *Add DuckDuckGo for Chrome?* Window, select *Add Extension.*



Add "DuckDuckGo for Chrome"?

★★★★★ (224)

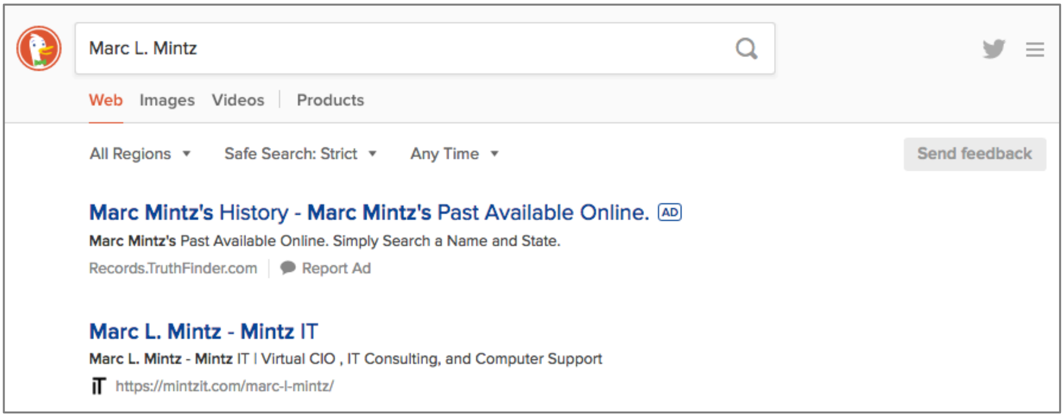
601,838 users

Open in Web Store

It can:

- Read and change your data on all duckduckgo.com sites and duckduckgo.com
- Change your search settings to: duckduckgo.com

5. To verify DuckDuckGo is the new default search engine, perform a search in Chrome. Note the Duck logo.



Marc Mintz's History - Marc Mintz's Past Available Online. AD

Marc Mintz's Past Available Online. Simply Search a Name and State.

Records.TruthFinder.com | Report Ad

Marc L. Mintz - Mintz IT

Marc L. Mintz - Mintz IT | Virtual CIO , IT Consulting, and Computer Support

https://mintzit.com/marc-l-mintz/

From now on, your default search engine for Chrome will be *DuckDuckGo*, hiding your search activities.

14.5 Clear History

By default, every browser maintains a full history of every site you have visited. Should someone gain access to your device, they will be able to view your browsing history.

You just realized that: 1) Your mother is coming over, 2) you have been naughty on the web all day, 3) you did not turn on Private Browsing, and 4) your mom will feel insulted if you insist that an account for her must to be created instead of accepting her protest: *Oh, baby, I only need to check my AOL email. Just let me get on your account for a minute.*

Is it time to panic?

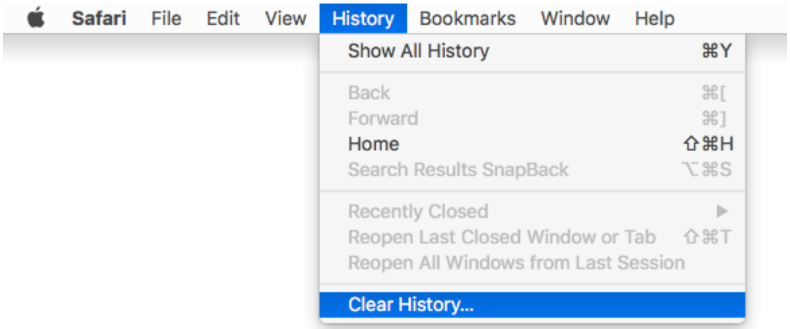
Not yet! You can erase your entire (steamy) browsing history in one click.

14.5.1 Assignment: Clear the Safari History

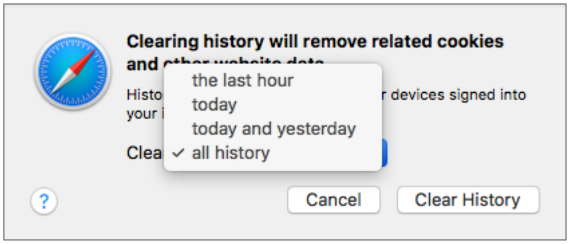
In this assignment, you clear your entire browsing history in Safari.

- Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Safari, and then select the *History* menu > *Clear History…*



2. A dialog box opens asking for what time frame you wish to clear your history. Make your selection, and then select the *Clear History* button.



Clearing history will remove related cookies and

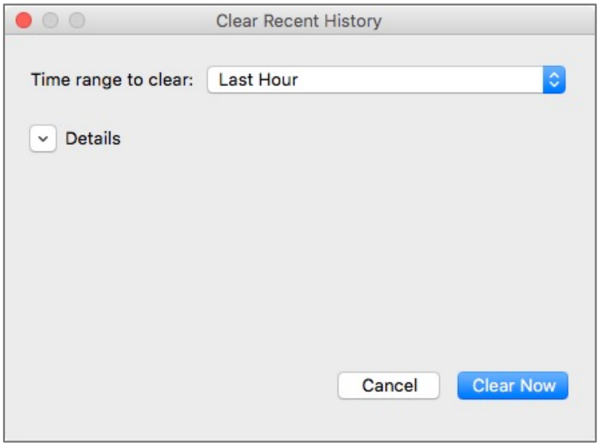
The Safari history is now cleared as you defined.

14.5.2 Assignment: Clear the Firefox Browsing History

In this assignment, you clear your Firefox browsing history.

Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

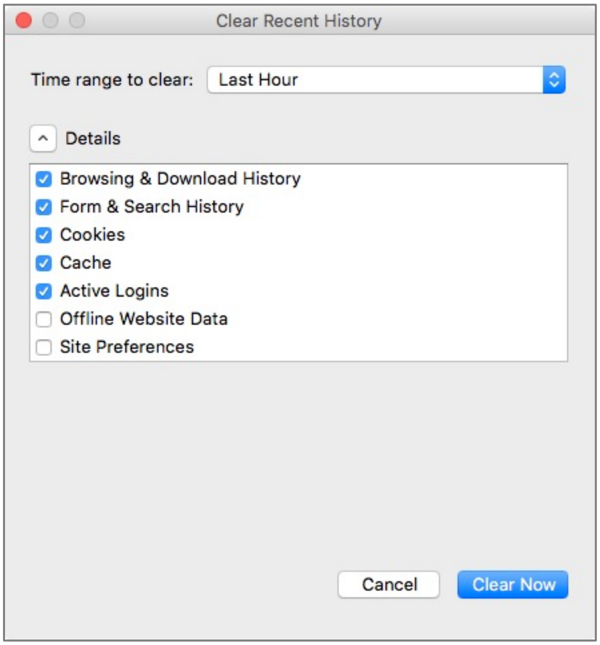
1. Open Firefox.
2. Select the *History* menu > *Clear Recent History*… The *Clear All History* window opens.



Clear Recent History

Time range to clear: Last Hour

3. Select the *Details* disclosure button to expand your options.



Clear Recent History

Time range to clear: Last Hour

Details

☑ Browsing & Download History
☑ Form & Search History
☑ Cookies
☑ Cache
☑ Active Logins
☐ Offline Website Data
☐ Site Preferences

4. Select the *Time range to clear,* which history items are to be cleared, and then click the *Clear Now.*
5. Close the *Clear Recent History* window.

The Firefox history is now history.

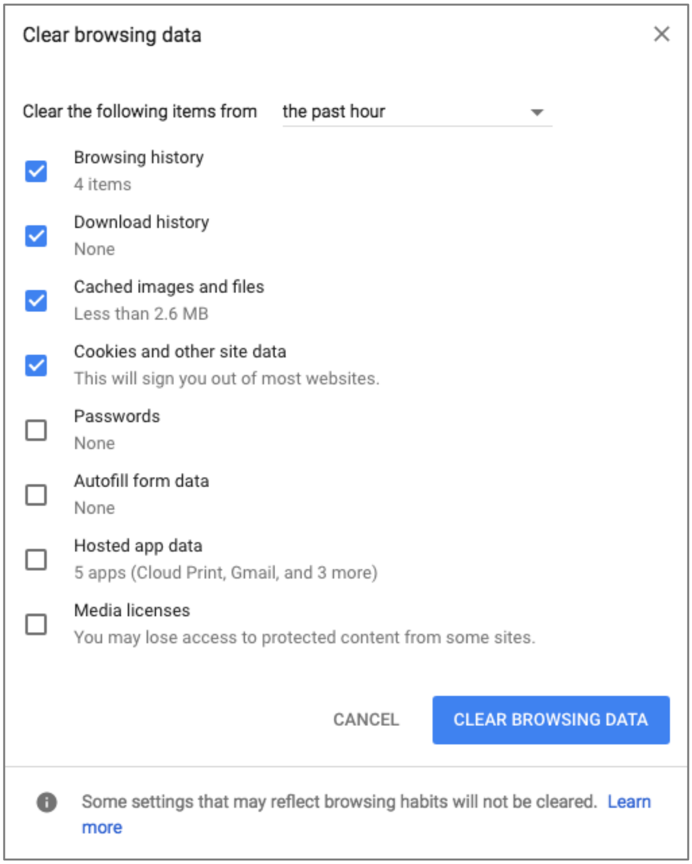
14.5.3 Assignment: Clear the Chrome History

In this assignment, you clear your browsing history in Chrome.

- Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Chrome.

2. Select the *Chrome* menu > *Clear Browsing Data…* The *Clear Browsing Data* window opens.



Clear browsing data

Clear the following items from the past hour

☑ Browsing history
4 items

☑ Download history
None

☑ Cached images and files
Less than 2.6 MB

☑ Cookies and other site data
This will sign you out of most websites.

□ Passwords
None

□ Autofill form data
None

□ Hosted app data
5 apps (Cloud Print, Gmail, and 3 more)

□ Media licenses
You may lose access to protected content from some sites.

Some settings that may reflect browsing habits will not be cleared. Learn more

3. Select which items are to be cleared, and then click the *Clear Browsing data* button.

Done!

14.6 Browser Plug-Ins

One of the great advances in personal computer software development was the concept of plug-ins or extensions[6]. These small strings of code add functionality to the host application. In the case of web browsers, this may be anything from the ability to encrypt web-based email, to viewing proprietary video formats.

The bad news about plug-ins is that they run with the full power of the host application. This means that a malicious plug-in may have the power to secretly redirect your web browser to fake websites (such as a phony copy of your bank), or harvest all your passwords, monitor your purchases, etc.

There are many malicious plug-ins. It is vital to only install those plug-ins that you need to install, to know which plug-ins are installed, and to rid yourself of unnecessary plug-ins.

14.6.1 Assignment: Install TrafficLight Plug-In for Safari

In this assignment, you search for extensions for Safari, and then install the *TrafficLight* anti-malicious website extension.

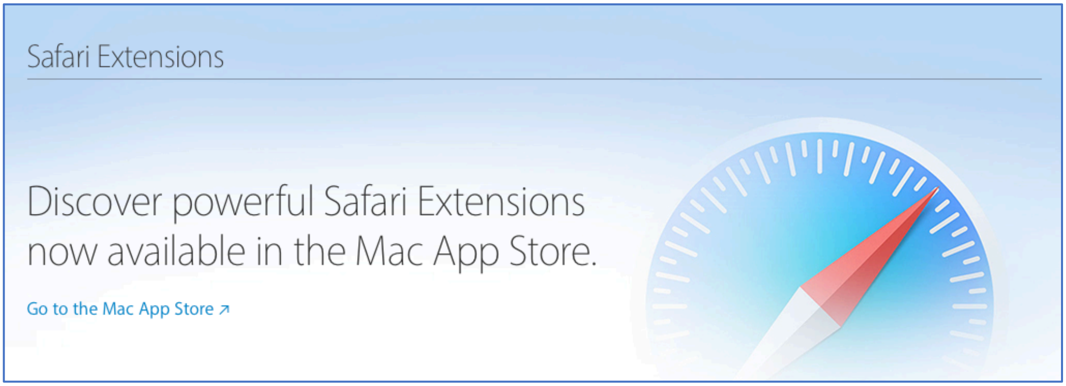
- Note: Prior to macOS 10.13, Safari Extensions were found in a separate area of the Apple website. Starting with macOS 10.13, Safari Extensions are moving to the Mac App Store. As of this writing, Apple was in transition with how to acquire and install Safari Extensions, with almost all Safari Extensions still found on the Apple site, and none on the Mac App Store.

1. Open Safari.

[6] *https://en.wikipedia.org/wiki/Plug-in_(computing)*

2. Select the *Safari* menu > *Safari Extensions…* The *Safari Extensions* page opens. Scroll down to see the featured Extensions located on the Apple Safari Extensions site. You may also search for Extensions in this area.

3. Assuming Apple will quickly migrate Extensions to the Mac App Store, Select *Go to the Mac App Store.*

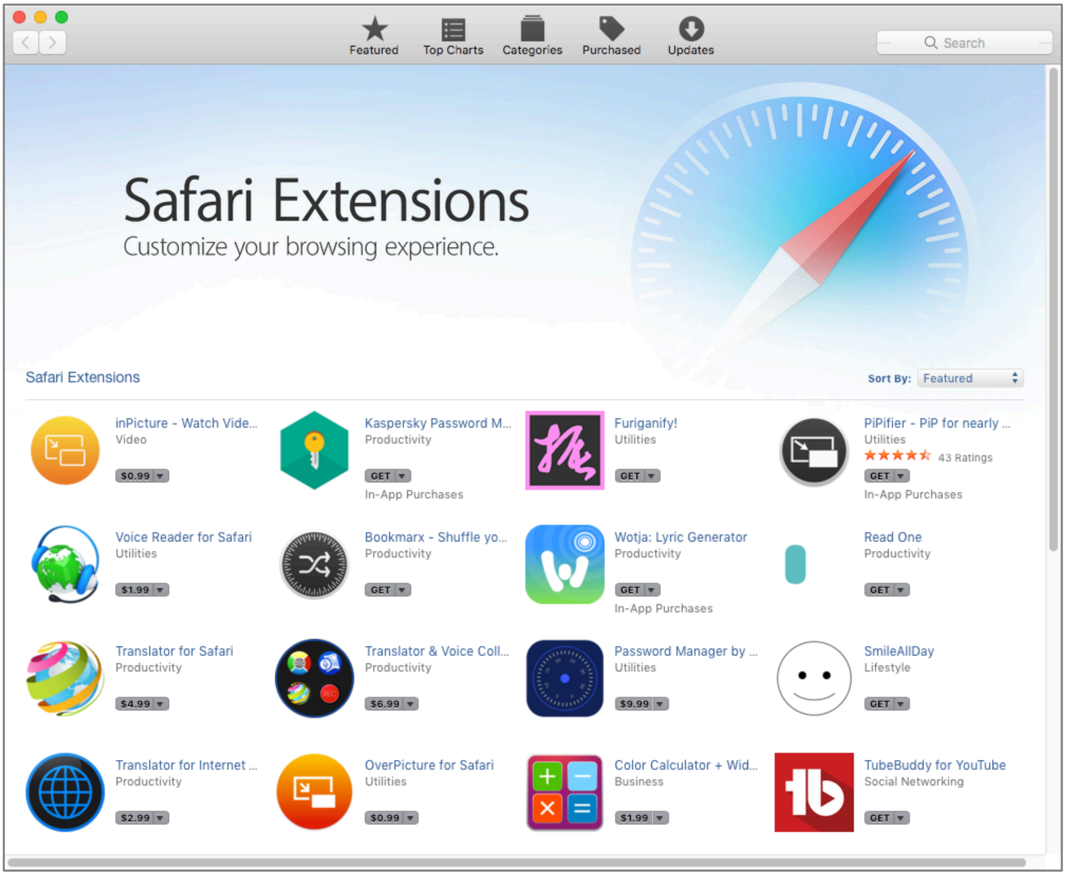


Safari Extensions

Discover powerful Safari Extensions now available in the Mac App Store.

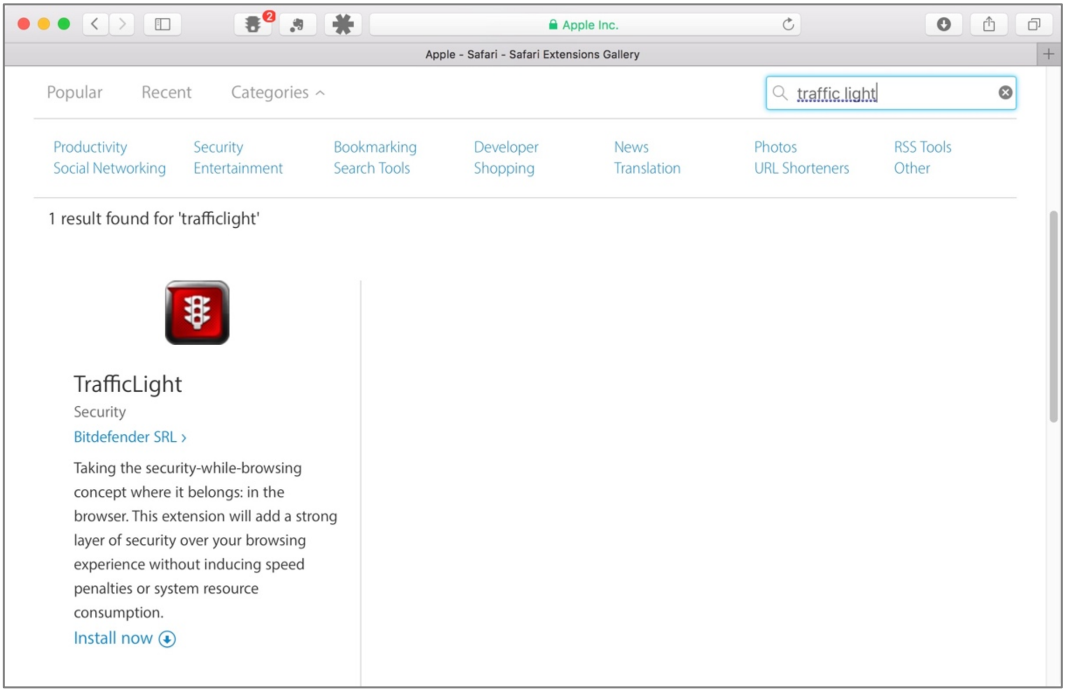
Go to the Mac App Store ↗

4. The Mac App Store opens to *Safari Extensions*. Select the *Popular, Recent,* or *Categories* links to explore the available *Safari Extensions*.



5. Explore and review some of the available extensions.

6. In the *Search* field, enter *TrafficLight*, and then tap the *Return* key. The *TrafficLight from Bitdefender* page opens. TrafficLight is a browser extension that adds protection from malicious websites. If you happen upon a compromised or malicious site, it will alert you and provide a button to back out of the site before your system is penetrated.



1 result found for 'trafficlight'

TrafficLight

Security

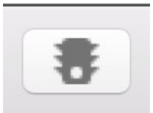
Bitdefender SRL ›

Taking the security-while-browsing concept where it belongs: in the browser. This extension will add a strong layer of security over your browsing experience without inducing speed penalties or system resource consumption.

Install now

7. Select the *Install now* link located under the description of TrafficLight.

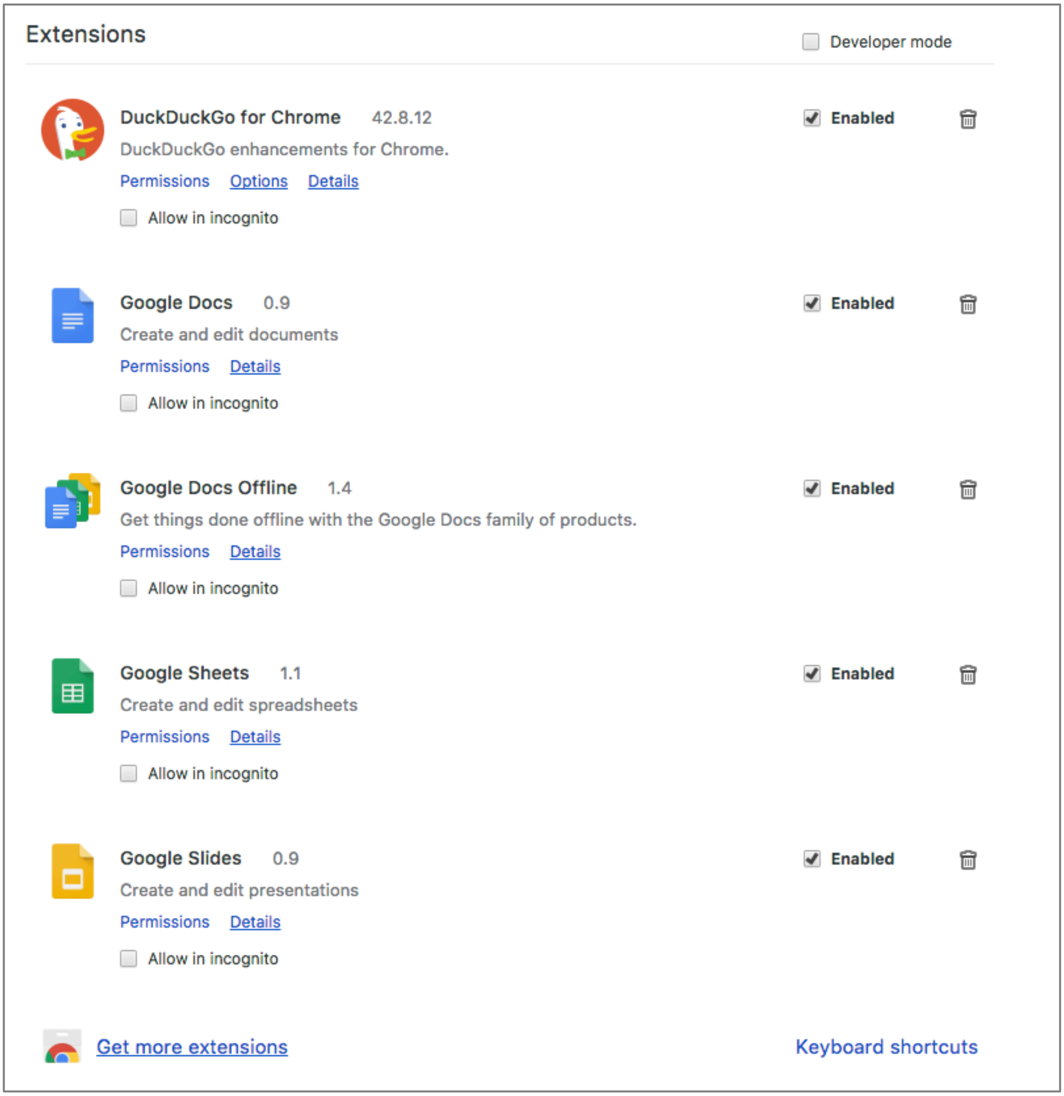
8. When installation completes, you will see a traffic light icon in your Safari tool bar.



14.6.2 Assignment: Install TrafficLight Plug-In for Google Chrome

In this assignment, you search for extensions for Chrome, and install the *TrafficLight* anti-malicious website extension.

1. Open Google Chrome.
2. Select the *Menu* icon (3 lines at the right edge of the tool bar) > *More Tools* > *Extensions.* Any currently installed extensions will display.



Extensions

□ Developer mode

DuckDuckGo for Chrome 42.8.12

DuckDuckGo enhancements for Chrome.

Permissions Options Details

□ Allow in incognito

☑ Enabled

Google Docs 0.9

Create and edit documents

Permissions Details

□ Allow in incognito

☑ Enabled

Google Docs Offline 1.4

Get things done offline with the Google Docs family of products.

Permissions Details

□ Allow in incognito

☑ Enabled

Google Sheets 1.1

Create and edit spreadsheets

Permissions Details

□ Allow in incognito

☑ Enabled

Google Slides 0.9

Create and edit presentations

Permissions Details

□ Allow in incognito

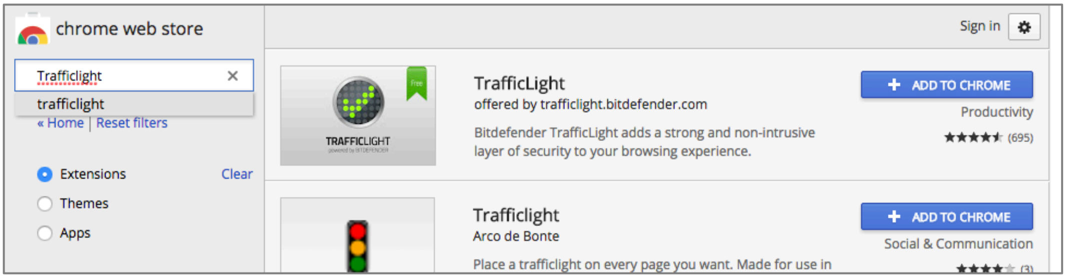
☑ Enabled

Get more extensions

Keyboard shortcuts

3. Scroll to the bottom of the page, and then select Get *More Extensions.*
4. Explore the available extensions.

5. In the sidebar, select *Extensions,* in the *Search the store* field, enter *TrafficLight*, and then tap the *Return* or *Enter* key. The results page appears.



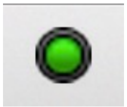
TrafficLight
offered by trafficlight.bitdefender.com
Bitdefender TrafficLight adds a strong and non-intrusive layer of security to your browsing experience.
Productivity
★★★★★ (695)

Trafficlight
Arco de Bonte
Place a trafficlight on every page you want. Made for use in
Social & Communication
★★★★☆ (3)

6. In the *TrafficLight offered by trafficlight Bitdefender* area, select the *Add To Chrome* button. If prompted to confirm, confirm the addition.

7. At the *Add TrafficLight?* Window, select *Add extension.*

8. Once installed, you will see the TrafficLight icon in the Chrome tool bar–a green dot.



14.6.3 Assignment: Install TrafficLight For Firefox

In this assignment, you search for plug-ins for Firefox, and install the *TrafficLight* anti-malicious website extension.

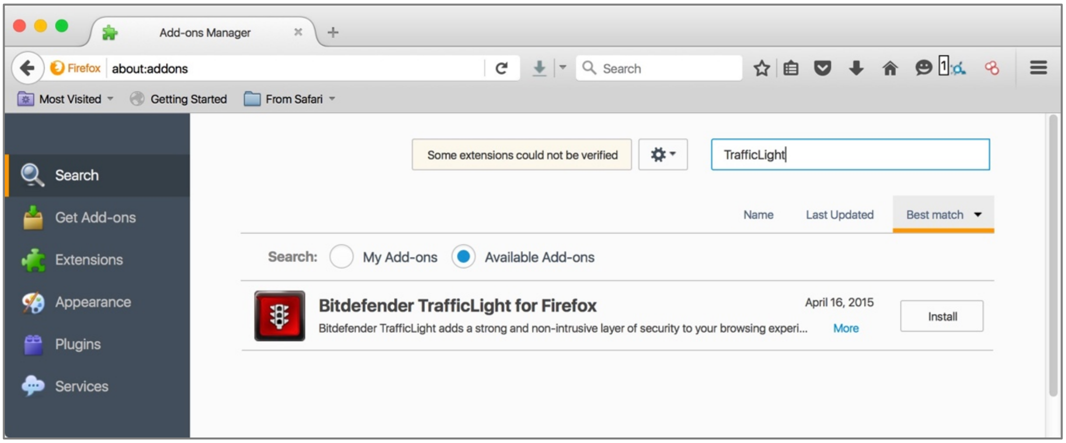
1. Open Firefox.

2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons.*

3. Select *Get Add-ons* from the left sidebar.

4. Explore the available add-ons.

5. In the *Search all add-ons* field, enter *TrafficLight*, and then tap the *Return* key. The results page appears.



Some extensions could not be verified

TrafficLight

Search: ○ My Add-ons ● Available Add-ons

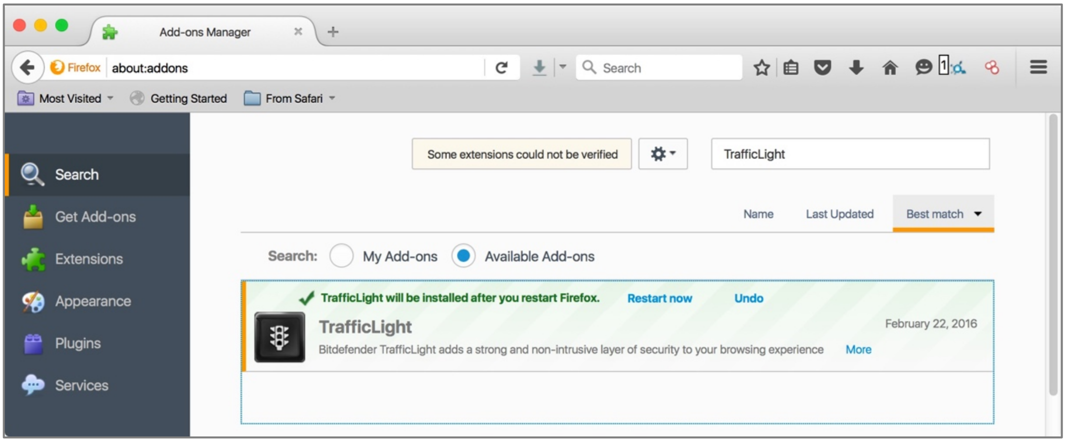
Bitdefender TrafficLight for Firefox — April 16, 2015

Bitdefender TrafficLight adds a strong and non-intrusive layer of security to your browsing experi...

6. In the Bitdefender TrafficLight for Firefox area, select the Install button.

7. At the confirmation window, confirm OK.

8. Once installed, select the Restart now link.



Some extensions could not be verified

TrafficLight

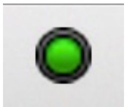
Search: ○ My Add-ons ● Available Add-ons

✓ TrafficLight will be installed after you restart Firefox.

TrafficLight — February 22, 2016

Bitdefender TrafficLight adds a strong and non-intrusive layer of security to your browsing experience

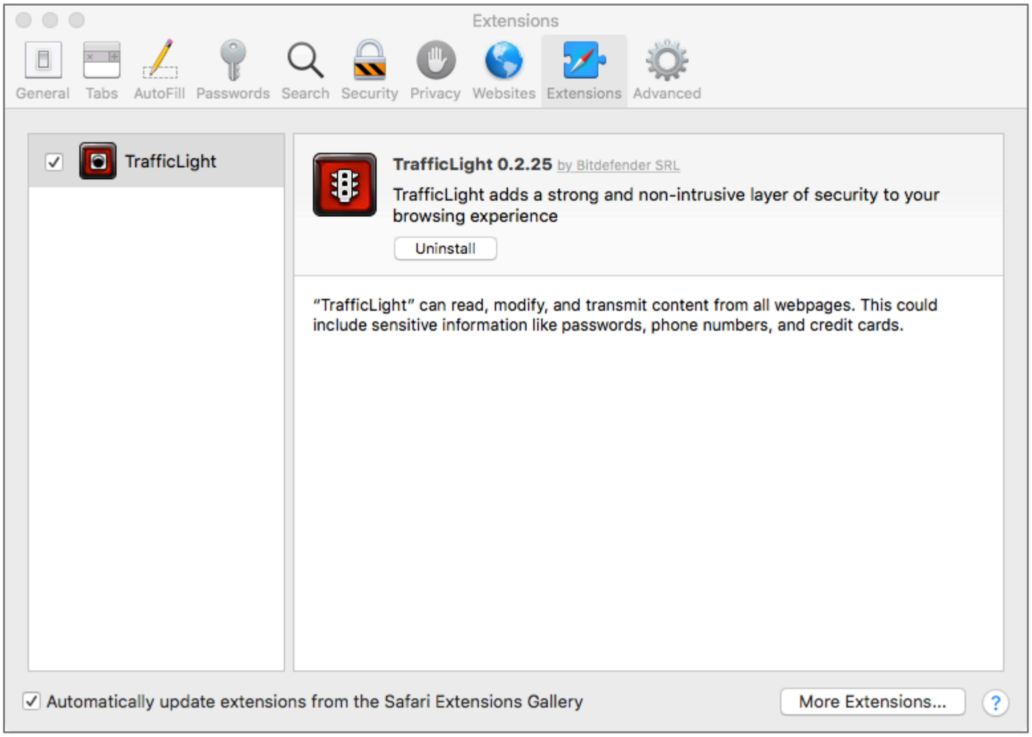
9. Once installed, you will see the TrafficLight icon in the Chrome tool bar–a green dot.



14.6.4 Assignment: Find and Remove Extensions from Safari

In this assignment, you see the installed Safari Extensions, determine if they are what you need, and remove those that are not needed.

1. Open Safari.
2. Select the *Safari* menu > *Preferences.*
3. From the Preferences tool bar, select *Extensions.*



☑ TrafficLight

TrafficLight 0.2.25 by Bitdefender SRL

TrafficLight adds a strong and non-intrusive layer of security to your browsing experience

"TrafficLight" can read, modify, and transmit content from all webpages. This could include sensitive information like passwords, phone numbers, and credit cards.

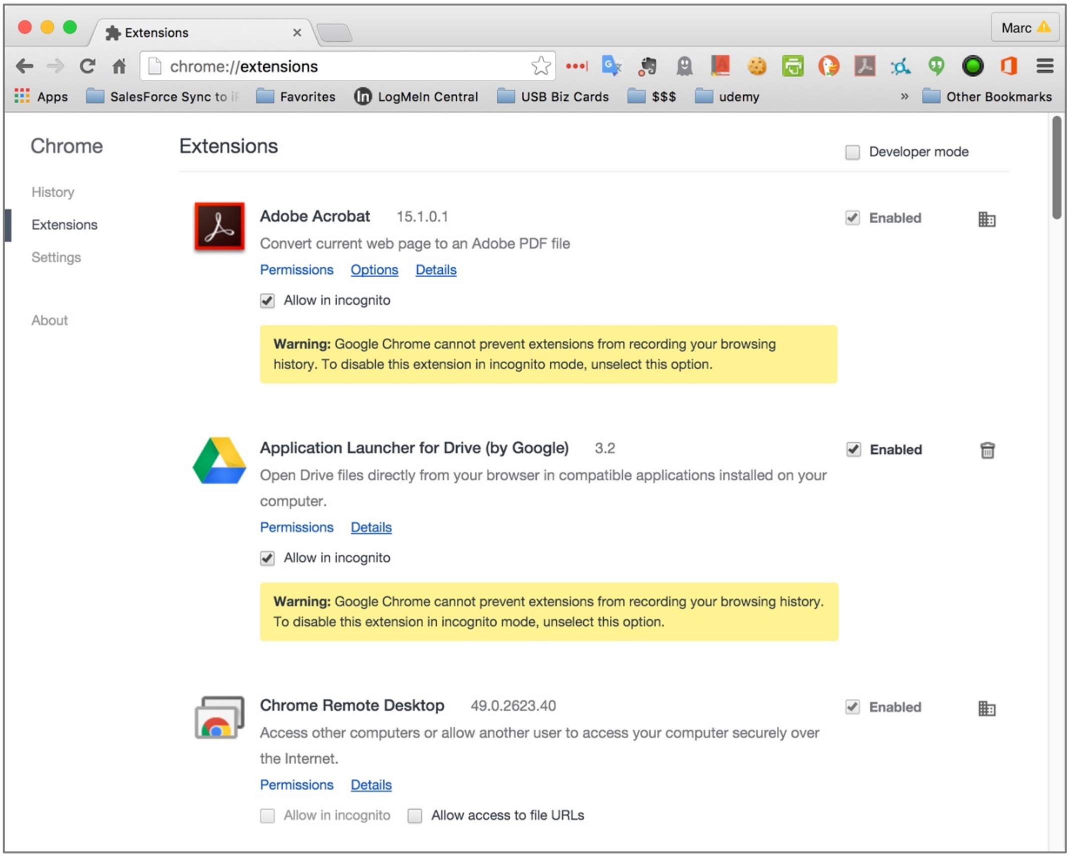
☑ Automatically update extensions from the Safari Extensions Gallery

4. All currently installed Extensions will display in the sidebar.
5. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
6. If you determine you don't want any Extensions installed, select the target Extension in the sidebar, and then select the *Uninstall* button under the target extension.

14.6.5 Assignment: Find and Remove Extensions from Chrome

In this assignment, you see the installed Chrome Extensions, determine if they are what you need, and remove those that are not needed.

1. Open Chrome.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Settings*.
3. Select *Extensions* from the left sidebar. The *Chrome Extensions* page opens.



Extensions

□ Developer mode

Adobe Acrobat 15.1.0.1
Convert current web page to an Adobe PDF file
Permissions Options Details
☑ Allow in incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in incognito mode, unselect this option.
☑ Enabled

Application Launcher for Drive (by Google) 3.2
Open Drive files directly from your browser in compatible applications installed on your computer.
Permissions Details
☑ Allow in incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in incognito mode, unselect this option.
☑ Enabled

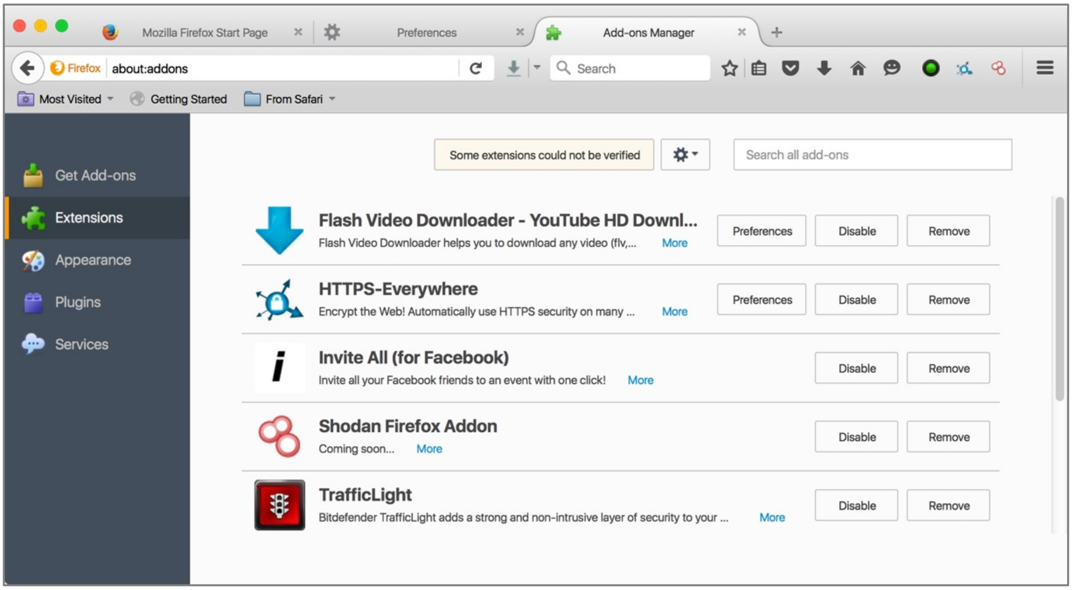
Chrome Remote Desktop 49.0.2623.40
Access other computers or allow another user to access your computer securely over the Internet.
Permissions Details
□ Allow in incognito □ Allow access to file URLs
☑ Enabled

4. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
5. If you determine you don't want any Extensions installed, click the *Trash* icon to the far right.

14.6.6 Assignment: Find and Remove Add-Ons from Firefox

In this assignment, you see the installed Firefox Extensions, determine if they are what you need to be installed, and remove those that are not needed.

1. Open Firefox.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons.*
3. Select *Extensions* from the left sidebar.



Flash Video Downloader - YouTube HD Downl...
Flash Video Downloader helps you to download any video (flv,...

HTTPS-Everywhere
Encrypt the Web! Automatically use HTTPS security on many ...

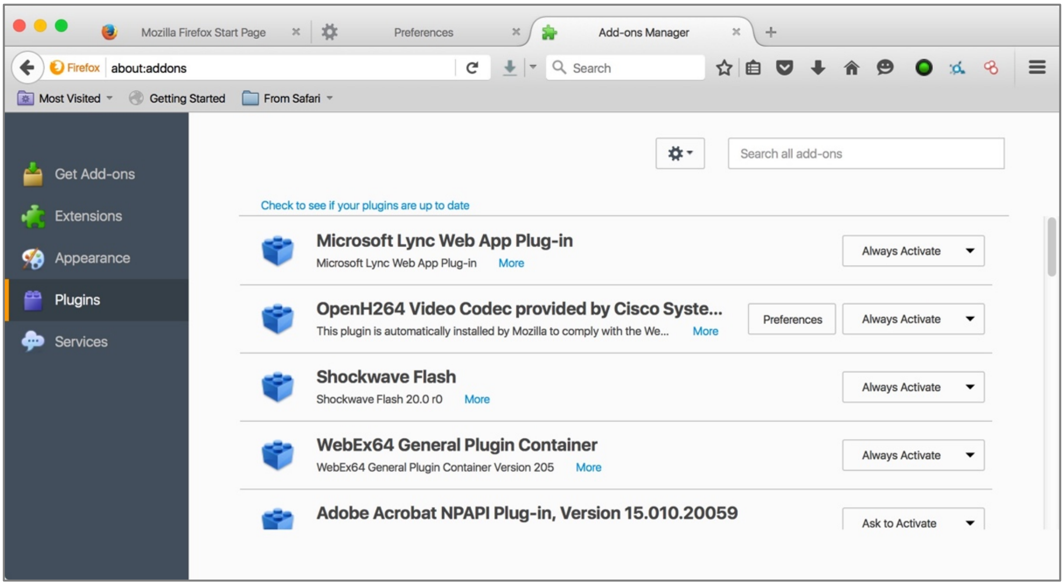
Invite All (for Facebook)
Invite all your Facebook friends to an event with one click!

Shodan Firefox Addon
Coming soon...

TrafficLight
Bitdefender TrafficLight adds a strong and non-intrusive layer of security to your ...

6. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
7. If you determine you don't want any Extensions installed, click the *Remove* button to the far right.

8. Select *Plugins* from the left sidebar.



Check to see if your plugins are up to date

Microsoft Lync Web App Plug-in
Microsoft Lync Web App Plug-in

OpenH264 Video Codec provided by Cisco Syste...
This plugin is automatically installed by Mozilla to comply with the We...

Shockwave Flash
Shockwave Flash 20.0 r0

WebEx64 General Plugin Container
WebEx64 General Plugin Container Version 205

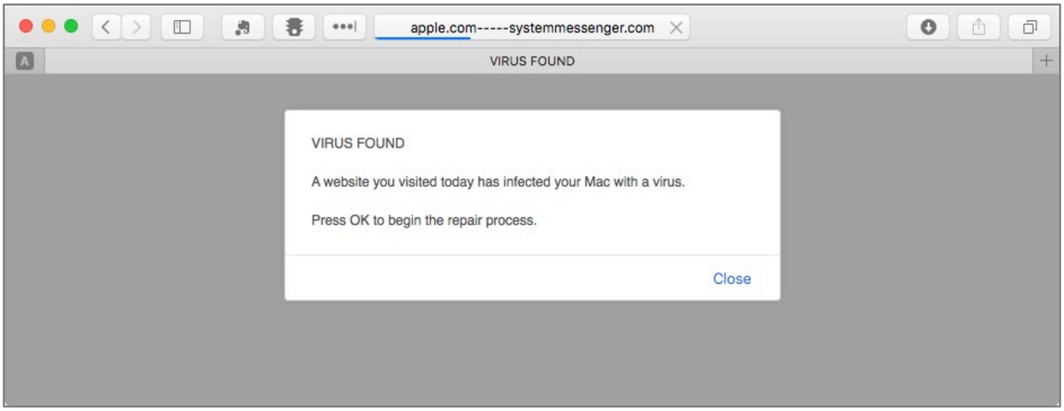
Adobe Acrobat NPAPI Plug-in, Version 15.010.20059

9. Perform an Internet search on any plugins that are unfamiliar to you. If you determine you don't want one active, select *Never Activate* from the pop-up menu to the far right.

14.7 Fraudulent Websites

As of this writing, there are over 1,000,000,000 active websites[7]. Within that, there may be millions of fraudulent websites. Of the diverse types of fraud found on the Internet[8], among the most common are websites that misrepresent who they are. This may be in the form of appearing like Bank of America, but with a URL of perhaps http://bankofamerica.cm, instead of the true http://bankofamerica.com. In this case, the criminal is hoping for someone to make the typo. Once at their site, you would enter your account and password as typical. The difference is that this time, the criminal now has your credentials–and all your money within minutes.

As a side note, in this specific example as of the time of this writing, this URL actually *is* as scam site. But not for the scheme mentioned. When I went to *http://bankofamerica.cm*, I was routed to the following:



VIRUS FOUND

A website you visited today has infected your Mac with a virus.

Press OK to begin the repair process.

If we look at the full URL, it is: http://apple.com-----systemmessenger.com/dgkg/?city=Albuquerque&region=New%20Mexico&country=US&ip=71.222.135.33&isp=Qwest%20Communications%20Company%20Llc&os=OS%20X&osv=OS%20X%2010.11%20El%20Capitan&browser=Safari&browserversion=Safari%209&voluumdata=BASE64dmlkLi4wMDAwMDAwNi01Yzg0LTRjNjYtODAwMC0wMDAwMDAwMDAwMDBfX3ZwaWQuLmRl…

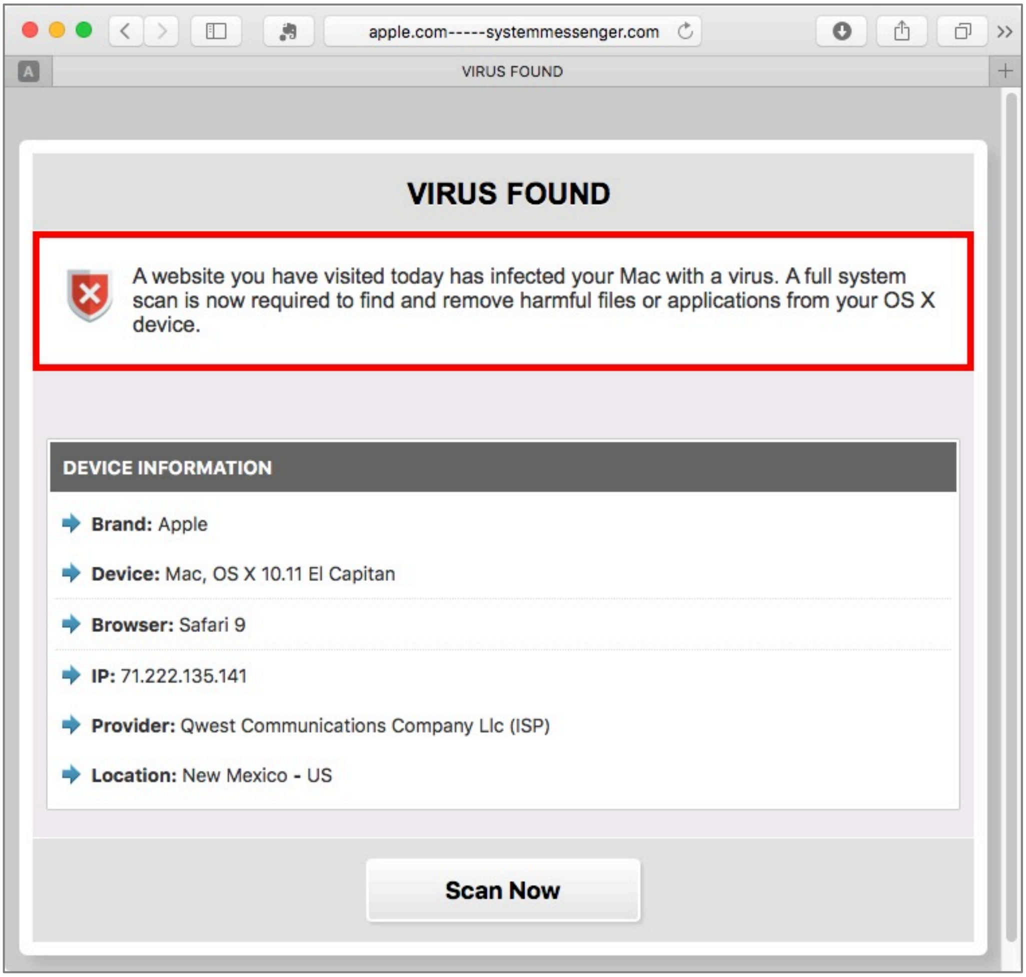
[7] *http://www.internetlivestats.com/total-number-of-websites/*
[8] *https://en.wikipedia.org/wiki/Internet_fraud*

From this URL, we can see that the criminal site attempts to appear as though it is Apple reporting that I have a virus.

They have also discerned my city, state, IP address, Internet provider (Qwest Communications), that I am using OS X 10.11 El Capitan, with Safari version 9.

If I were the typical user, I'd probably think there was a virus present and press the *OK* button as recommended. You may have also noticed the criminal was bright enough to do all of this, but not bright enough to put an *OK* button in the script!

So, I press the *Close* button. I'm presented with a new window:



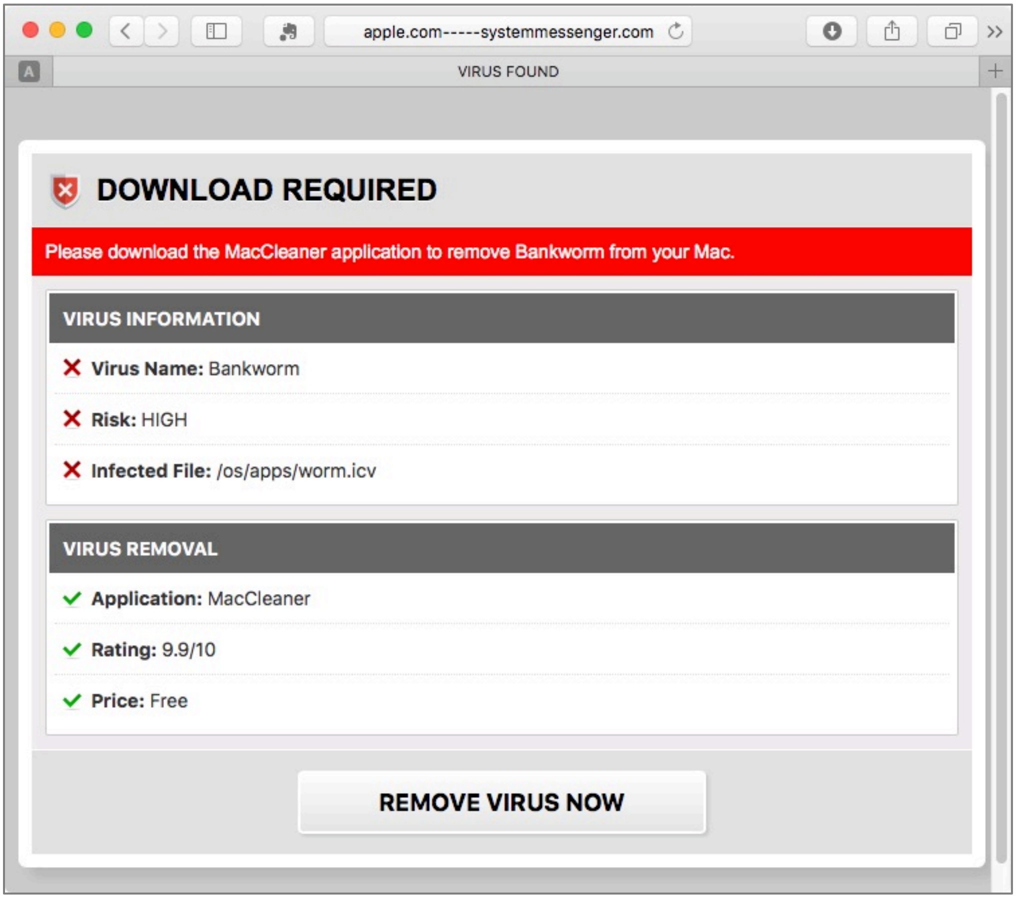
VIRUS FOUND

A website you have visited today has infected your Mac with a virus. A full system scan is now required to find and remove harmful files or applications from your OS X device.

DEVICE INFORMATION

- **Brand:** Apple
- **Device:** Mac, OS X 10.11 El Capitan
- **Browser:** Safari 9
- **IP:** 71.222.135.141
- **Provider:** Qwest Communications Company Llc (ISP)
- **Location:** New Mexico - US

Hey, who needs an *OK* button when the *Close* button will do the intended scam! So, let's see what happens when clicking the *Scan Now* button:



DOWNLOAD REQUIRED

Please download the MacCleaner application to remove Bankworm from your Mac.

VIRUS INFORMATION

✗ **Virus Name:** Bankworm

✗ **Risk:** HIGH

✗ **Infected File:** /os/apps/worm.icv

VIRUS REMOVAL

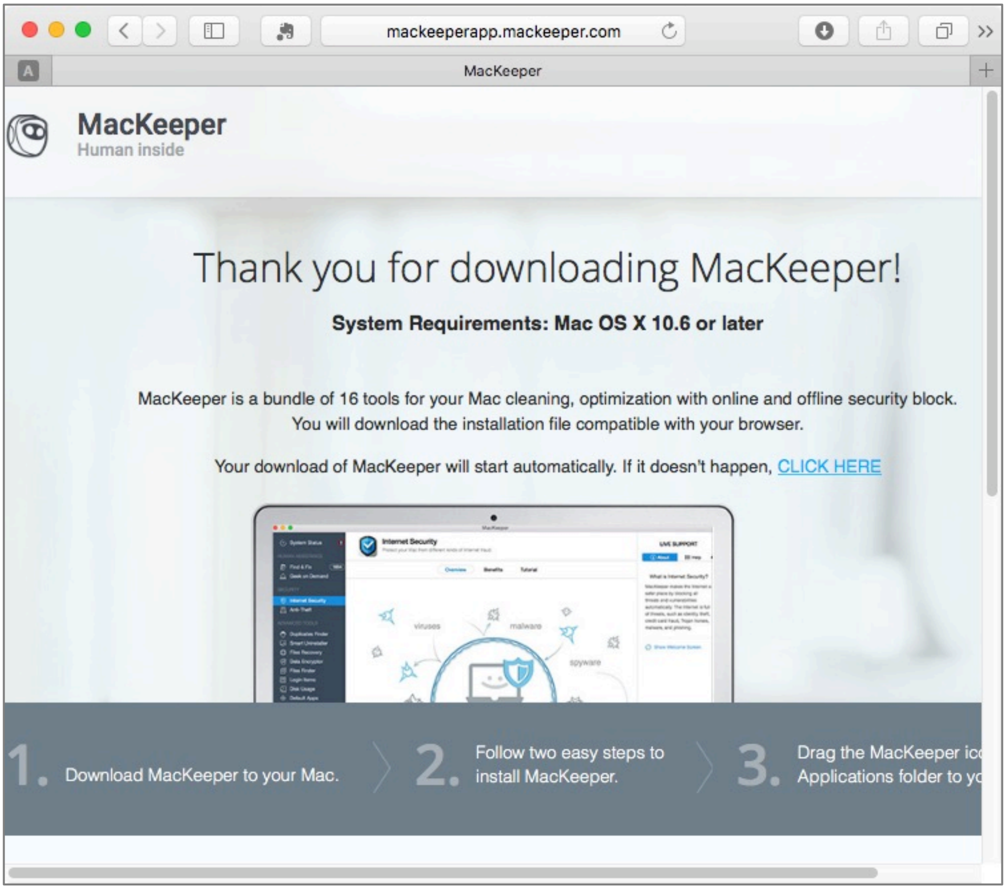
✓ **Application:** MacCleaner

✓ **Rating:** 9.9/10

✓ **Price:** Free

Appears they think I am infected with the *Bankworm* virus (which may or may not be a real malware name), and the infected file is in /os/apps/worm.icv. The only real problem I see is that there is no such file, and no such directory.

But they are offering a free solution to my non-existent problem. Let’s see where that takes us by clicking the *Remove Virus Now* button:



Thank you for downloading MacKeeper!

System Requirements: Mac OS X 10.6 or later

MacKeeper is a bundle of 16 tools for your Mac cleaning, optimization with online and offline security block. You will download the installation file compatible with your browser.

Your download of MacKeeper will start automatically. If it doesn't happen, CLICK HERE

1. Download MacKeeper to your Mac.

2. Follow two easy steps to install MacKeeper.

3. Drag the MacKeeper ic Applications folder to yo

MacKeeper?! Really! This product lost a class action lawsuit for deceptively advertising its functionality[9].

If you have followed along so far, just trash the MacKeeper download.

So, how to protect yourself against fraudulent sites? We will go through the few steps that can be taken, but the most important tool is your awareness.

[9] *https://topclassactions.com/lawsuit-settlements/closed-settlements/94767-mackeeper-class-action-settlement/*

14.8 Do Not Track

Most websites track which pages you visit, how long you stay on each page, and other metrics to better understand their visitors. That is a little creepy. Imagine going to the library, and having a librarian looking over your shoulder as you scan the card catalogue, and records each of the books and pages you glanced at.

Now let's take the analogy further. You leave the library and go across town to have lunch, and then shop for shoes. You look around and the same librarian is still watching and recording not only everything you have eaten, but everything you looked at on the menu.

Later you go for a date, and the librarian is sitting right behind you in the theater, noting who you are with, what scenes you reacted to, and more.

Web browsing isn't much different–except the snoop is normally invisible in the form of *cookies*.

Any website can initiate cookies on your browser. These keep a record of the pages you visit on the site. But they have evolved to report all the other places you visit and things that you do. This is why you can visit Amazon, look up my books, quit the web browser, launch it, go to okcupid, and see an ad for my books!

No, I'm not doing it, Amazon is. They know that you were interested in my book, and will prod you with images of it for a few days, assuming you will eventually succumb and buy.

There is the option to disable cookies, but most of your websites will demand they be enabled to visit the site.

Although there is no 100% solution to this intrusion, you can configure your browser to ask websites to not track your activities. And if you believe that works, I've got a bridge to sell you.

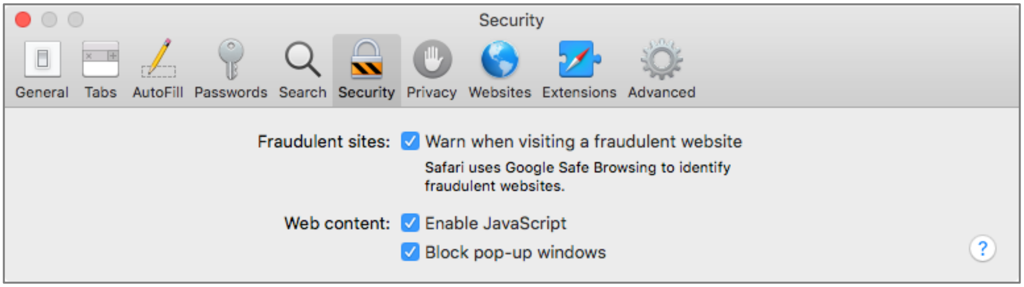
Ghostery

We can take *Do Not Track* to another level. To do this, we need to install a browser extension called *Ghostery*. Ghostery will display every tracker attempting to monitor your web activities, and gives you the ability to block them from garnering that information.

14.8.1 Assignment: Secure Safari

In this assignment, you secure Safari.

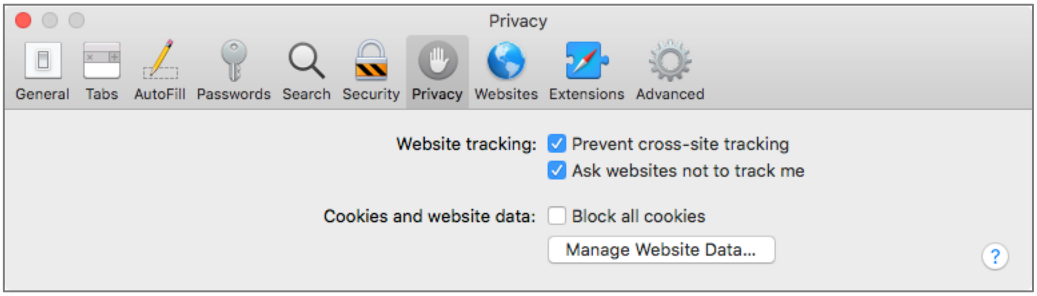
1. Open Safari, click the *Safari* menu > *Preferences* > *Security*.
2. Enable *Warn when visiting a fraudulent website*.



Fraudulent sites: ☑ Warn when visiting a fraudulent website
Safari uses Google Safe Browsing to identify fraudulent websites.

Web content: ☑ Enable JavaScript
☑ Block pop-up windows

3. Select the *Privacy* tab.



Website tracking: ☑ Prevent cross-site tracking
☑ Ask websites not to track me

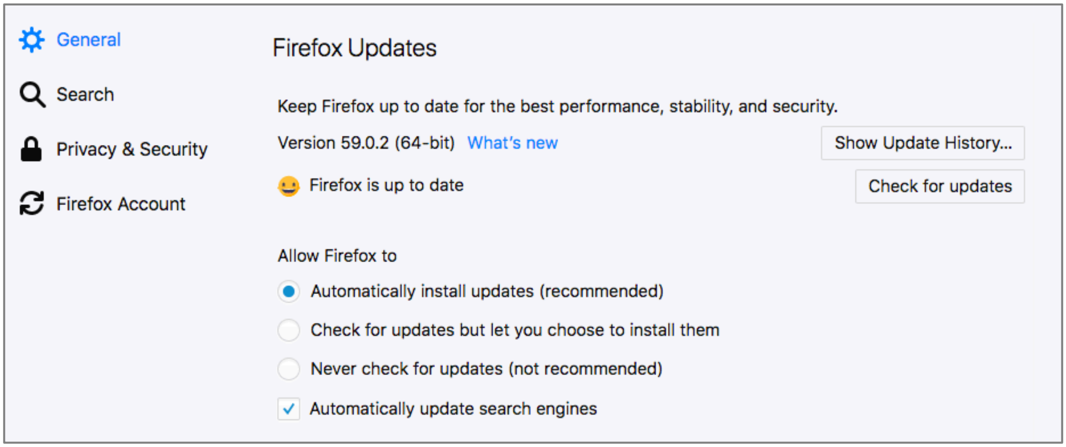
Cookies and website data: □ Block all cookies

4. Enable *Website tracking: Prevent cross-site tracking*
5. Enable *Website tracking: Ask websites not to track me.*
6. Close Safari Preferences.

14.8.2 Assignment: Secure Firefox

In this assignment, you secure Firefox.

1. Open Firefox, click the *Firefox menu* (three horizontal lines), and then select the *Preferences* button.
2. In the Preferences page, select *General* from the sidebar, and then scroll down to *Firefox Updates*. Set to *Automatically install updates.*



Firefox Updates

Keep Firefox up to date for the best performance, stability, and security.

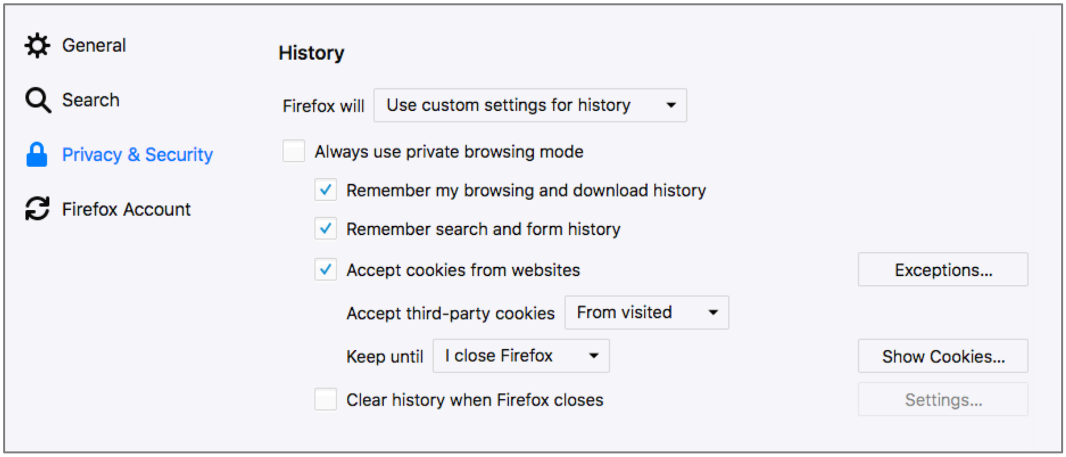
Version 59.0.2 (64-bit) What's new

Firefox is up to date

Allow Firefox to

● Automatically install updates (recommended)
○ Check for updates but let you choose to install them
○ Never check for updates (not recommended)
☑ Automatically update search engines

3. In the Preferences window, select on *Privacy & Security* in the left-hand pane, scroll down to *History,* and then select *Firefox will Use custom settings for history*. Configure to your taste, and here are my recommendations:



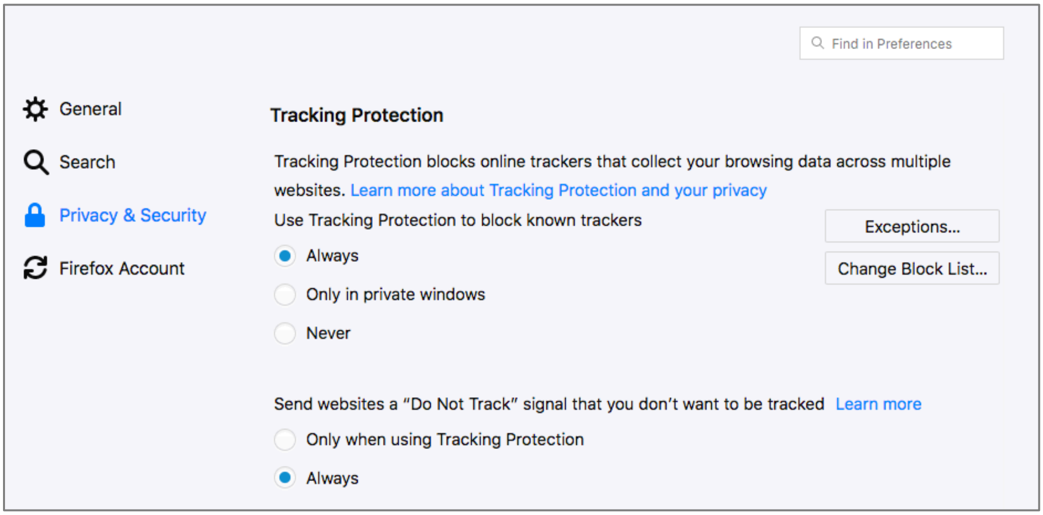
History

Firefox will: Use custom settings for history

□ Always use private browsing mode
☑ Remember my browsing and download history
☑ Remember search and form history
☑ Accept cookies from websites
Accept third-party cookies: From visited
Keep until: I close Firefox
□ Clear history when Firefox closes

4. Scroll down to the *Tracking Protection* area, enable *Use Tracking Protection to block known trackers Always.*

5. Set *Send websites a "Do Not Track" signal that you don't want to be tracked* to *Always.*



Tracking Protection

Tracking Protection blocks online trackers that collect your browsing data across multiple websites. Learn more about Tracking Protection and your privacy

Use Tracking Protection to block known trackers

● Always

○ Only in private windows

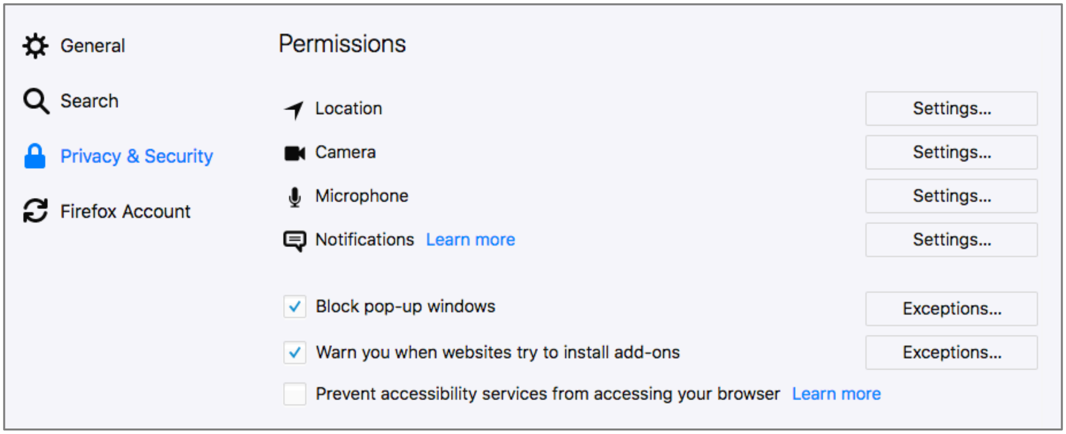
○ Never

Send websites a "Do Not Track" signal that you don't want to be tracked Learn more

○ Only when using Tracking Protection

● Always

6. Scroll down to *Permissions.* For *Location, Camera, Microphone,* and *Notifications,* select the *Settings* button. If there are sites listed to have access these services, remove them as desired.



Permissions

Location

Camera

Microphone

Notifications Learn more

☑ Block pop-up windows

☑ Warn you when websites try to install add-ons

□ Prevent accessibility services from accessing your browser Learn more

7. Enable *Block pop-up windows* to prevent them.
8. Enable *Warn you when websites try to install add-ons.*
9. Scroll down to *Security*. Enable *Block dangerous and deceptive content.*
10. Enable *Block dangerous downloads.*
11. Enable *Warn you about unwanted and uncommon software.*
12. Close Firefox Preferences.

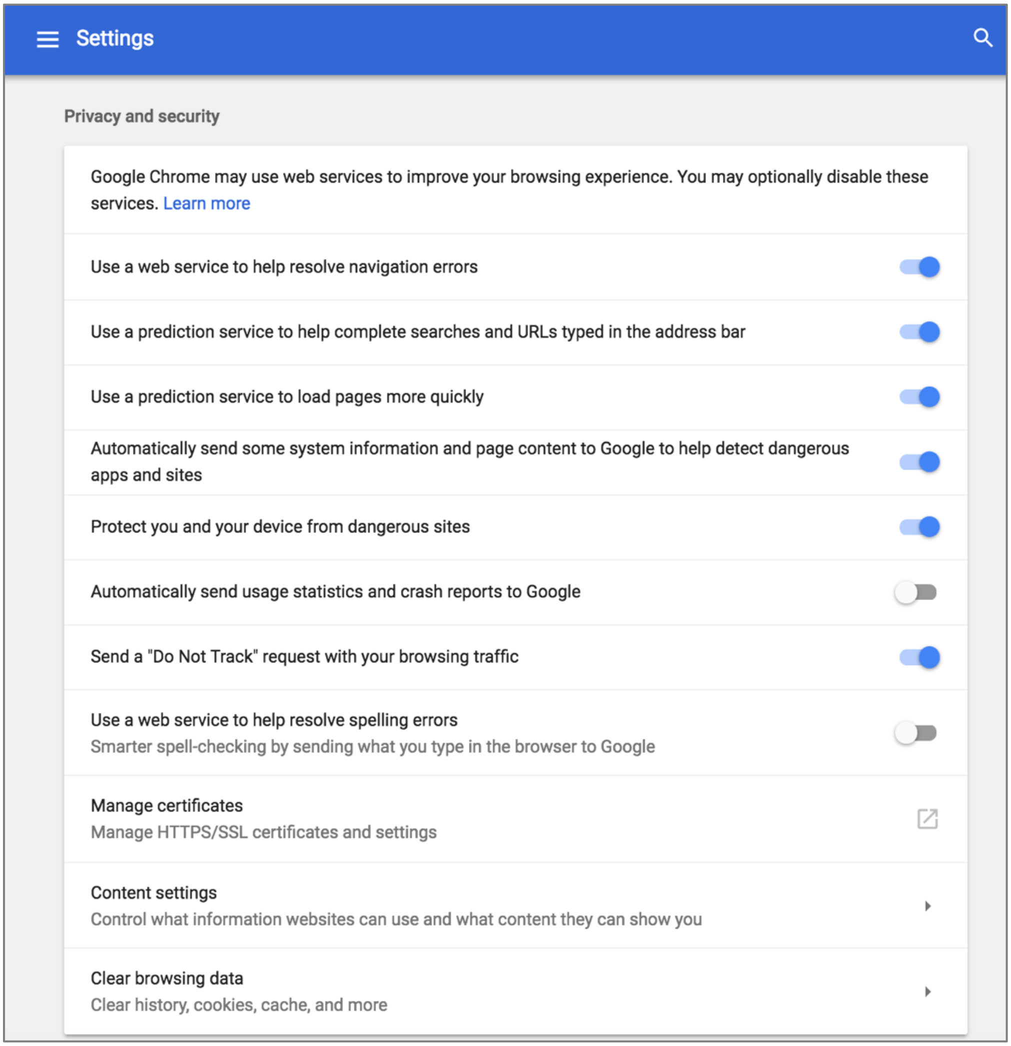
Congratulations. Your Firefox Browser is now secured from phishing attacks, third-party advertisers and known malware sites.

14.8.3 Assignment: Secure Chrome

Just as with Firefox, there are settings within Chrome that will keep you properly secured against the bad guys.

In this assignment, you secure Chrome

1. Open *Chrome*, select the menu item (3 dots), and then click *Settings.*
2. Click the 3 horizontal lines at the top left, select *Advanced,* and then select *Privacy & Security.* Recommended privacy and security settings are shown below:



Settings

Privacy and security

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

Use a web service to help resolve navigation errors ●

Use a prediction service to help complete searches and URLs typed in the address bar ●

Use a prediction service to load pages more quickly ●

Automatically send some system information and page content to Google to help detect dangerous apps and sites ●

Protect you and your device from dangerous sites ●

Automatically send usage statistics and crash reports to Google ○

Send a "Do Not Track" request with your browsing traffic ●

Use a web service to help resolve spelling errors ○
Smarter spell-checking by sending what you type in the browser to Google

Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

3. While you are here, have a look around and configure the rest of the *Privacy & Security* area.

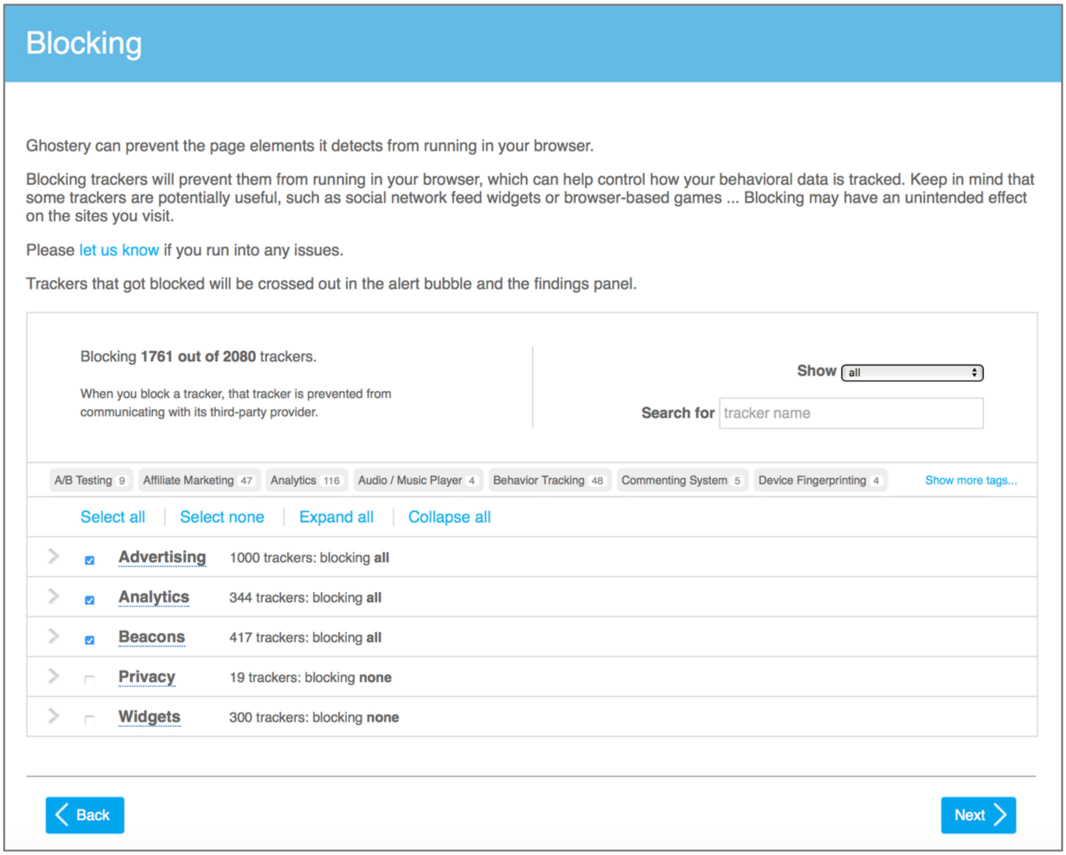
Congratulations. Your Chrome Browser is now securing from phishing attacks, third-party advertisers and known malware sites.

14.8.4 Assignment: Install Ghostery for Safari

In this assignment, you install the Ghostery extension for Safari, monitor who is monitoring you, and then block them.

1. Open Safari.
2. Browse to *https://ghostery.com*.
3. Select the *Install Ghostery* button. A link will download.
4. In your Downloads folder, locate and then double-click the *Ghostery.safariextz*.
5. In the *Ghostery is from the Safari Extension Gallery* window, select *Visit Gallery*.
6. In the *Safari Extensions* web page, select *Install now*.
7. The *Ghostery Introduction* page will open. Read the information, and then click the *Next* buttons.

8. At the *Notification* page, enable *Click here to enable Alert Bubble.* This will briefly display the trackers at each page visited. Then select *Next.*
9. At the *Blocking* page, select which trackers you want blocked, and then select the *Next* button. My recommended settings are shown below:



Blocking

Ghostery can prevent the page elements it detects from running in your browser.

Blocking trackers will prevent them from running in your browser, which can help control how your behavioral data is tracked. Keep in mind that some trackers are potentially useful, such as social network feed widgets or browser-based games ... Blocking may have an unintended effect on the sites you visit.

Please let us know if you run into any issues.

Trackers that got blocked will be crossed out in the alert bubble and the findings panel.

Blocking **1761 out of 2080** trackers.

When you block a tracker, that tracker is prevented from communicating with its third-party provider.

Show all

Search for tracker name

A/B Testing 9 | Affiliate Marketing 47 | Analytics 116 | Audio / Music Player 4 | Behavior Tracking 48 | Commenting System 5 | Device Fingerprinting 4 | Show more tags...

Select all | Select none | Expand all | Collapse all

☑ **Advertising** 1000 trackers: blocking **all**

☑ **Analytics** 344 trackers: blocking **all**

☑ **Beacons** 417 trackers: blocking **all**

□ **Privacy** 19 trackers: blocking **none**

□ **Widgets** 300 trackers: blocking **none**

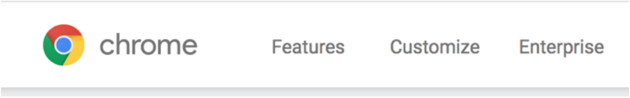
10. When complete, click the *Next* button, and then close the Ghostery page.
11. To test Ghostery, visit *https://slashdot.com.* Note the purple alerts that appear in the bottom right corner, and the new Ghostery icon in the toolbar.
12. Click the Ghostery icon in the toolbar to learn more about Ghostery, and to configure preferences.

From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.

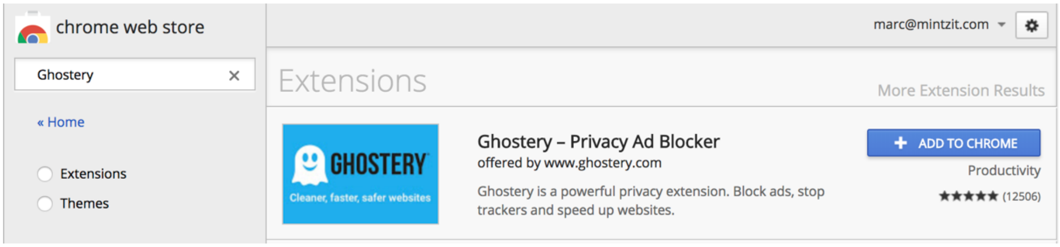
14.8.5 Assignment: Install Ghostery for Chrome

In this assignment, you install the Ghostery extension for Chrome, monitor who is monitoring you, and then block them.

1. Open Chrome.
2. Go to *https://chrome.google.com.*
3. Click *Customize* link at the top center of the window.



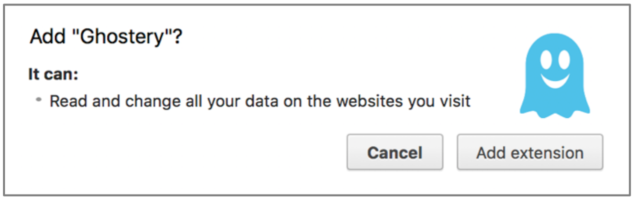
4. In the *Search the Store* field, enter *Ghostery*, and then tap the *Enter* or *Return* key. Extensions matching this search term will appear.



Ghostery – Privacy Ad Blocker
offered by www.ghostery.com

Ghostery is a powerful privacy extension. Block ads, stop trackers and speed up websites.

5. When Ghostery is found, click *ADD TO CHROME* button.
6. In the *Add "Ghostery"?* dialog, click *Add extension.*

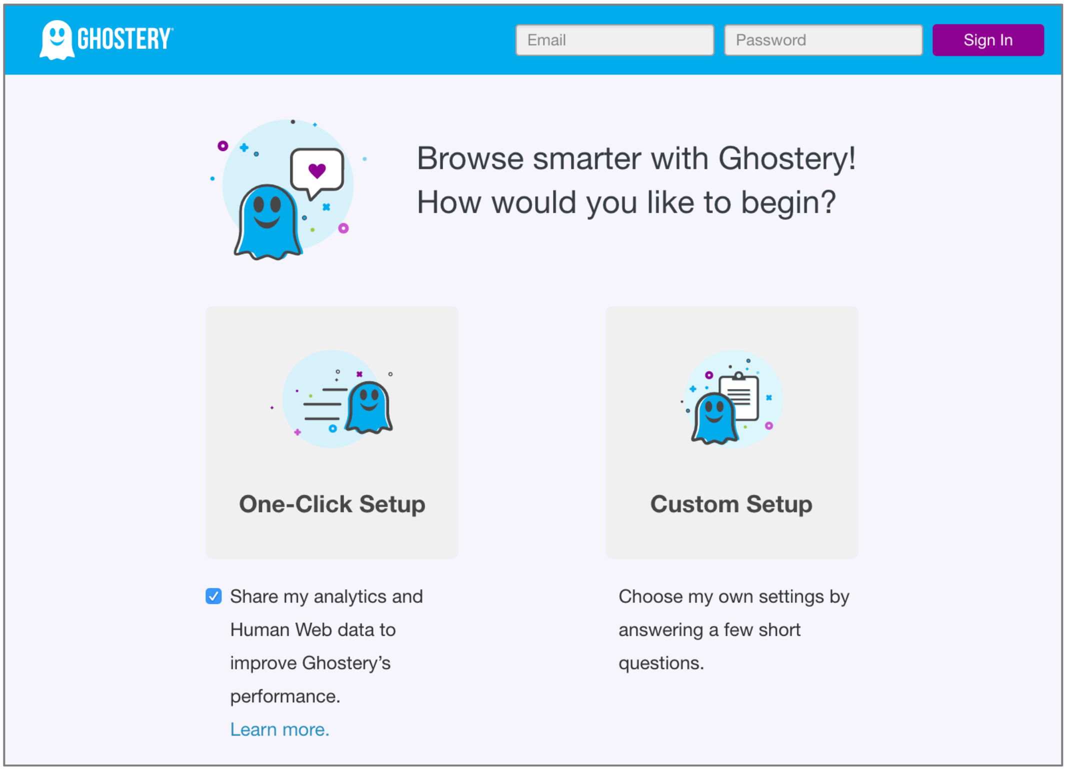


Add "Ghostery"?

It can:

- Read and change all your data on the websites you visit

7. Ghostery will display a few screens asking for your preferences. You may click the *One-Click Setup* button to automatically configure, or click *Custom Setup* to configure to your taste.

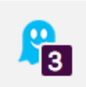


Browse smarter with Ghostery!
How would you like to begin?

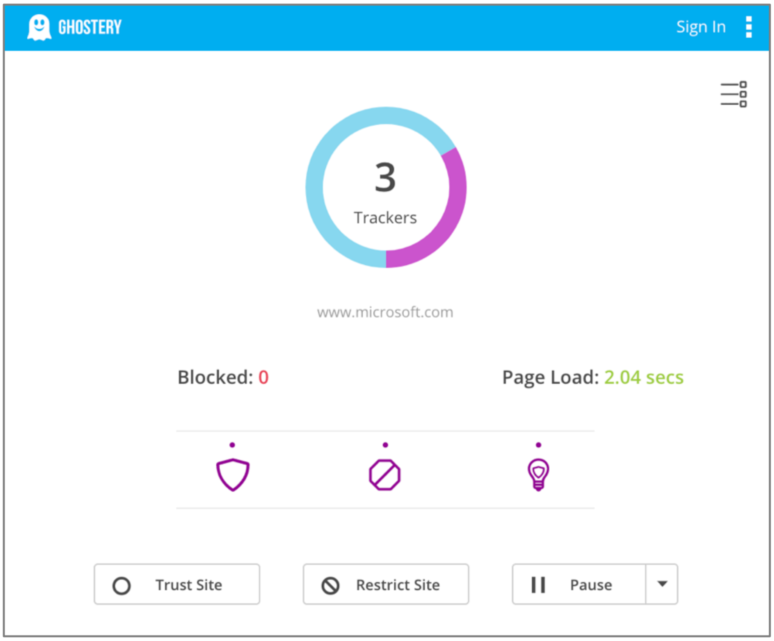
☑ Share my analytics and Human Web data to improve Ghostery's performance. Learn more.

Choose my own settings by answering a few short questions.

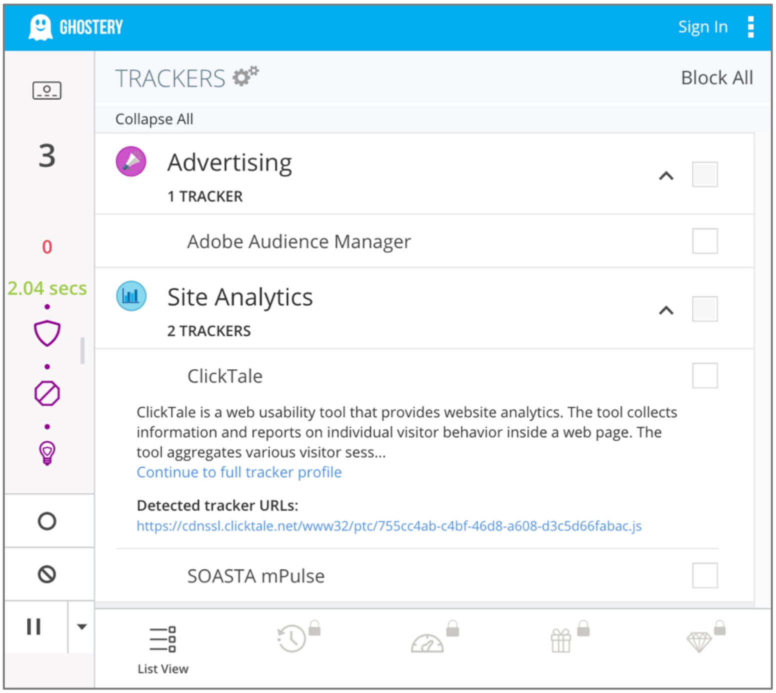
8. You may configure to your taste at this time, or do nothing. You can always configure later.
9. Notice that you now have the Ghostery icon in the Chrome Tool bar. In this example, it is notifying me that there are 3 trackers on the Ghostery page.



10. Click the Ghostery icon. This will display information about who is tracking you.



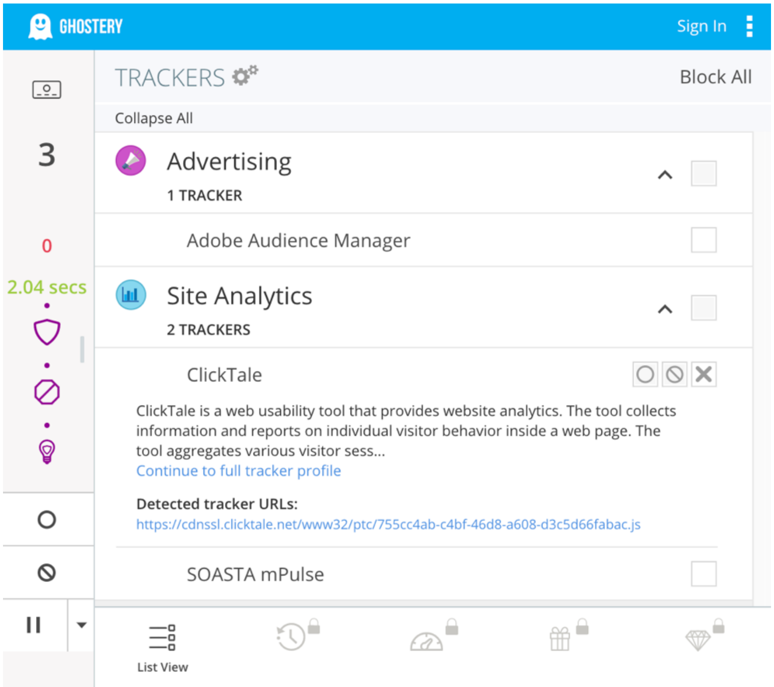
11. Click the *Detail View* icon under the *Sign in* link to display more information.
12. Click on one of the trackers to see details on it. In this example, *ClickTale.*



ClickTale is a web usability tool that provides website analytics. The tool collects information and reports on individual visitor behavior inside a web page. The tool aggregates various visitor sess...
Continue to full tracker profile

Detected tracker URLs:
https://cdnssl.clicktale.net/www32/ptc/755cc4ab-c4bf-46d8-a608-d3c5d66fabac.js

13. Hover your cursor to the right of one of the tracker names (in this example, *ClickTale*), and you now have icons allowing you to *Trust on this site, Block on this site,* and *Block on all sites.*



ClickTale is a web usability tool that provides website analytics. The tool collects information and reports on individual visitor behavior inside a web page. The tool aggregates various visitor sess...

Continue to full tracker profile

Detected tracker URLs:

https://cdnssl.clicktale.net/www32/ptc/755cc4ab-c4bf-46d8-a608-d3c5d66fabac.js

14. Click the 3-dot settings icon at the top right corner of the Ghostery window > *Settings*. Explore the options, and then configure to your taste.
15. Close Chrome.

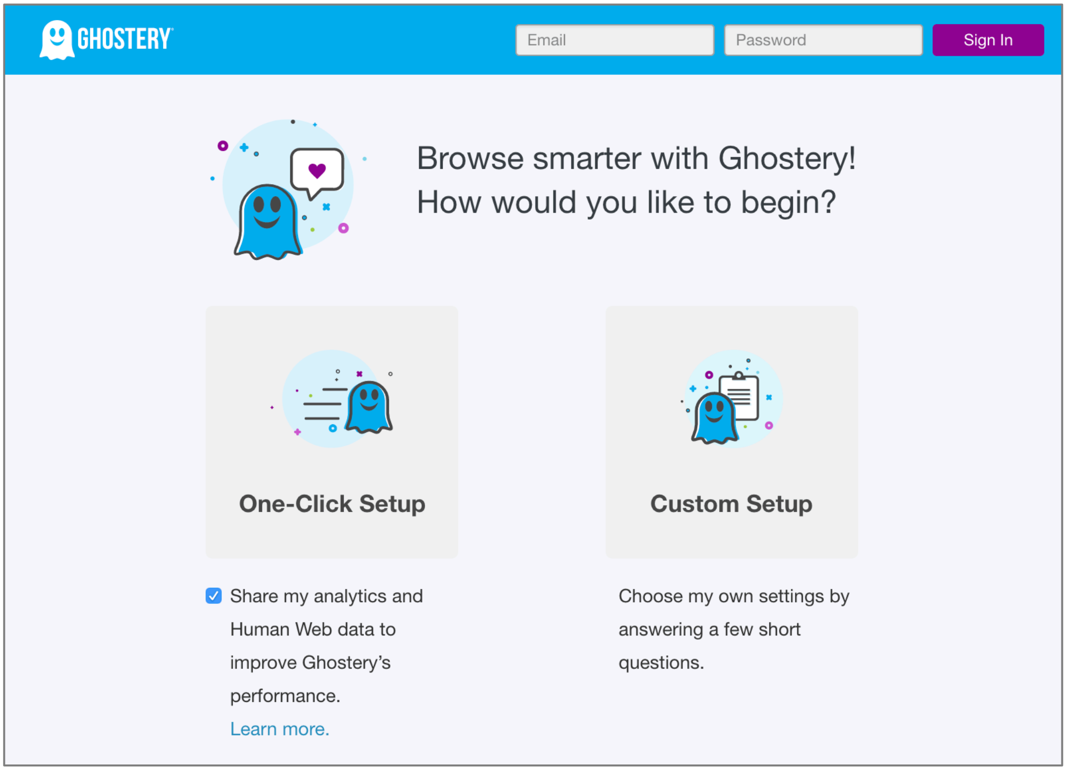
From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.

14.8.6 Assignment: Install Ghostery for Firefox

In this assignment, you install the Ghostery extension for Firefox, monitor who is monitoring you, and then block them.

1. Open Firefox.
2. Click the menu icon (three horizontal lines) > *Add-ons.*
3. From the sidebar, select *Extensions.*
4. In the *Search* field, enter *Ghostery.*

5. Select *Ghostery–Privacy Add Blocker.*
6. Click the *Add to Firefox* button.
7. At the *Add Ghostery Privacy Ad Blocker?* dialog box, click *Add.*
8. Ghostery will display a few screens asking for your preferences. You may click the *One-Click Setup* button to automatically configure, or click *Custom Setup* to configure to your taste.

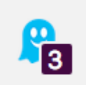


Browse smarter with Ghostery!
How would you like to begin?

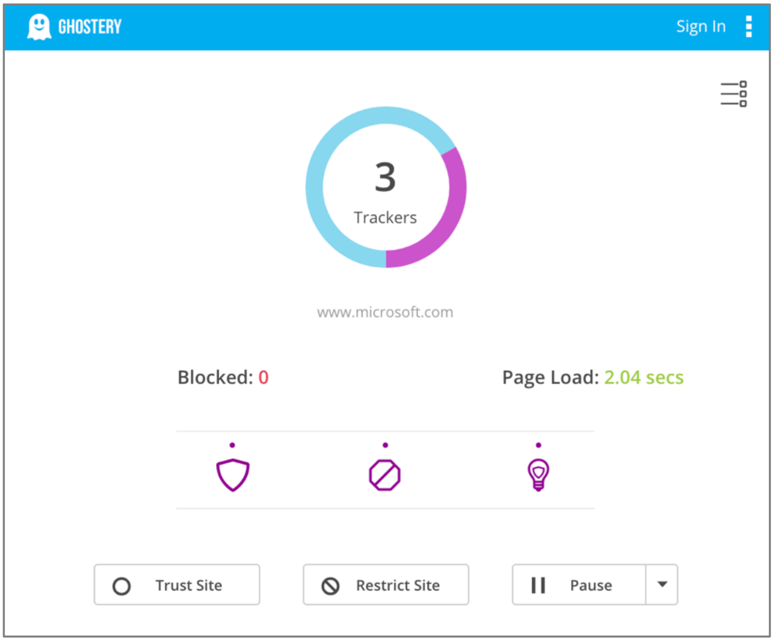
☑ Share my analytics and Human Web data to improve Ghostery's performance.
Learn more.

Choose my own settings by answering a few short questions.

9. You may configure to your taste at this time, or do nothing. You can always configure later.
10. Notice that you now have the Ghostery icon in the Chrome Tool bar. In this example, it is notifying me that there are 3 trackers on the Ghostery page.

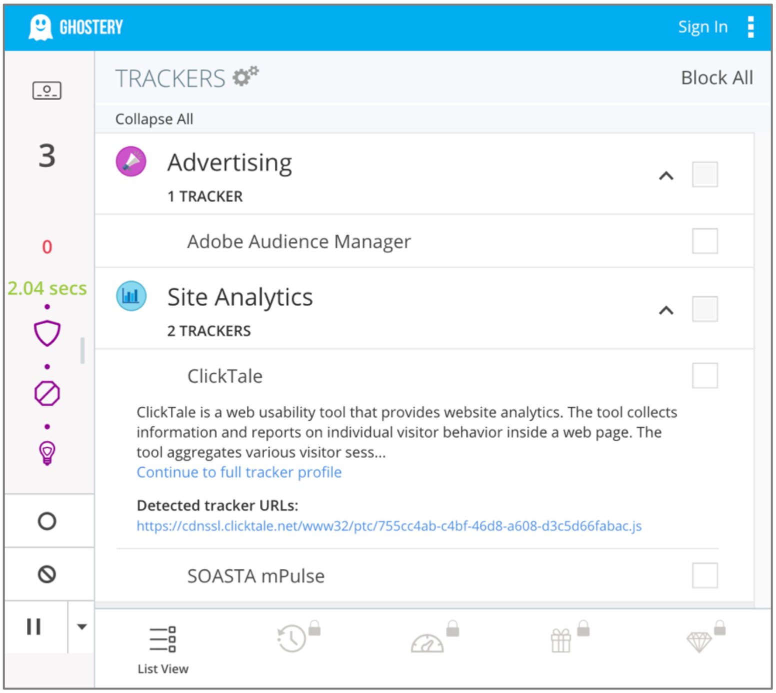


11. Click the Ghostery icon. This will display information about who is tracking you.



12. Click the *Detail View* icon under the *Sign in* link to display more information.

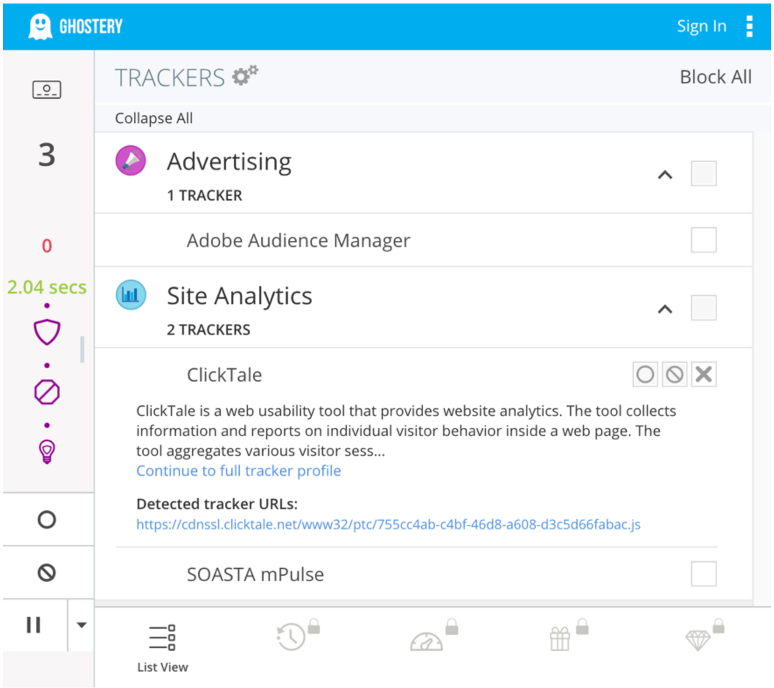
13. Click on one of the trackers to see details on it. In this example, *ClickTale*.



ClickTale is a web usability tool that provides website analytics. The tool collects information and reports on individual visitor behavior inside a web page. The tool aggregates various visitor sess...
Continue to full tracker profile

Detected tracker URLs:
https://cdnssl.clicktale.net/www32/ptc/755cc4ab-c4bf-46d8-a608-d3c5d66fabac.js

14. Hover your cursor to the right of one of the tracker names (in this example, *ClickTale*), and you now have icons allowing you to *Trust on this site, Block on this site,* and *Block on all sites.*



ClickTale is a web usability tool that provides website analytics. The tool collects information and reports on individual visitor behavior inside a web page. The tool aggregates various visitor sess...
Continue to full tracker profile

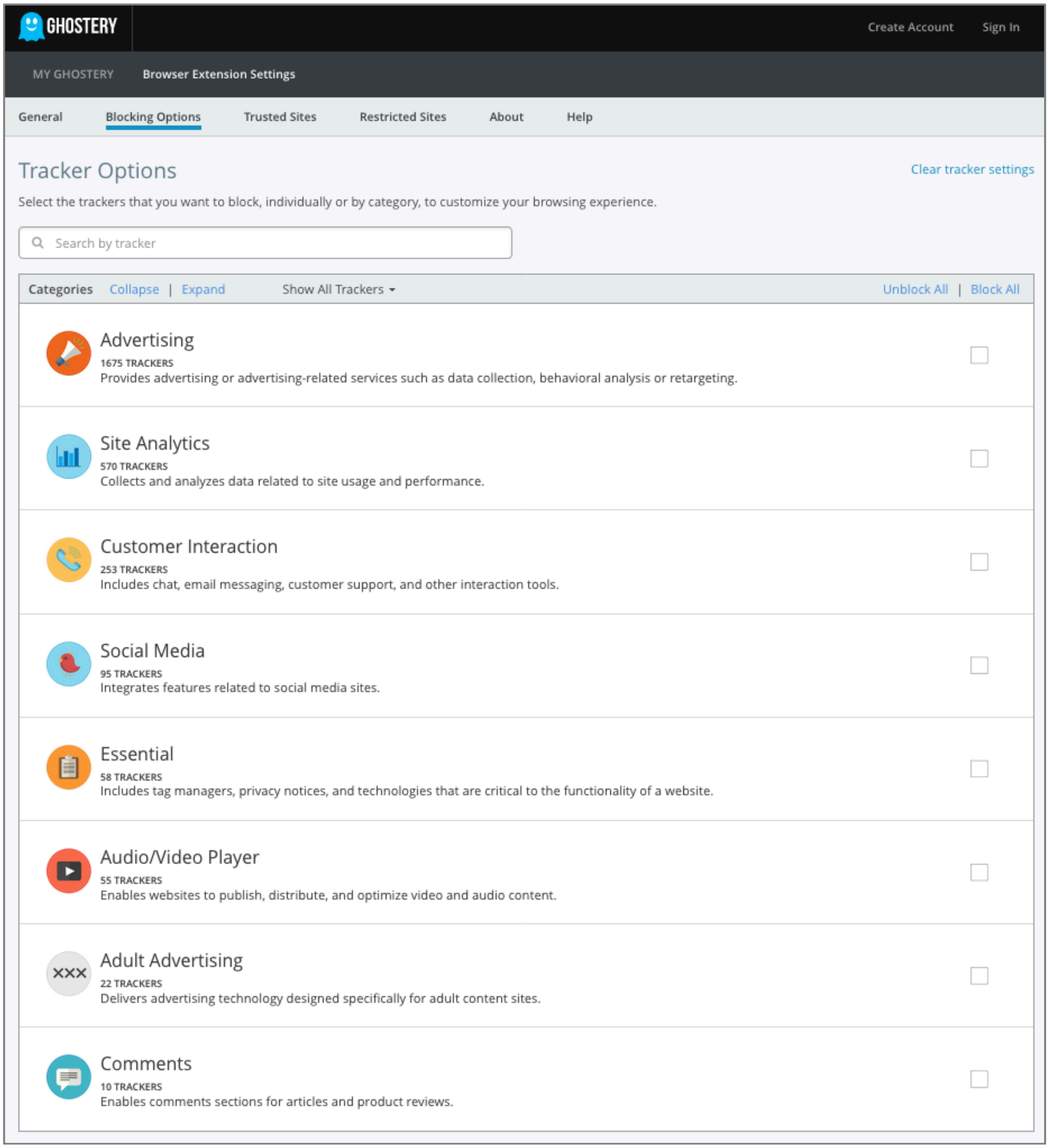
Detected tracker URLs:
https://cdnssl.clicktale.net/www32/ptc/755cc4ab-c4bf-46d8-a608-d3c5d66fabac.js

15. Click the 3-dot settings icon at the top right corner of the Ghostery window > *Settings*. Explore the options, and then configure to your taste.

16. Close Firefox.

From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.

17. At the *Tracker Options* page, select the trackers to be blocked.



Tracker Options

Clear tracker settings

Select the trackers that you want to block, individually or by category, to customize your browsing experience.

Search by tracker

Categories Collapse | Expand Show All Trackers ▾ Unblock All | Block All

Advertising
1675 TRACKERS
Provides advertising or advertising-related services such as data collection, behavioral analysis or retargeting. □

Site Analytics
570 TRACKERS
Collects and analyzes data related to site usage and performance. □

Customer Interaction
253 TRACKERS
Includes chat, email messaging, customer support, and other interaction tools. □

Social Media
95 TRACKERS
Integrates features related to social media sites. □

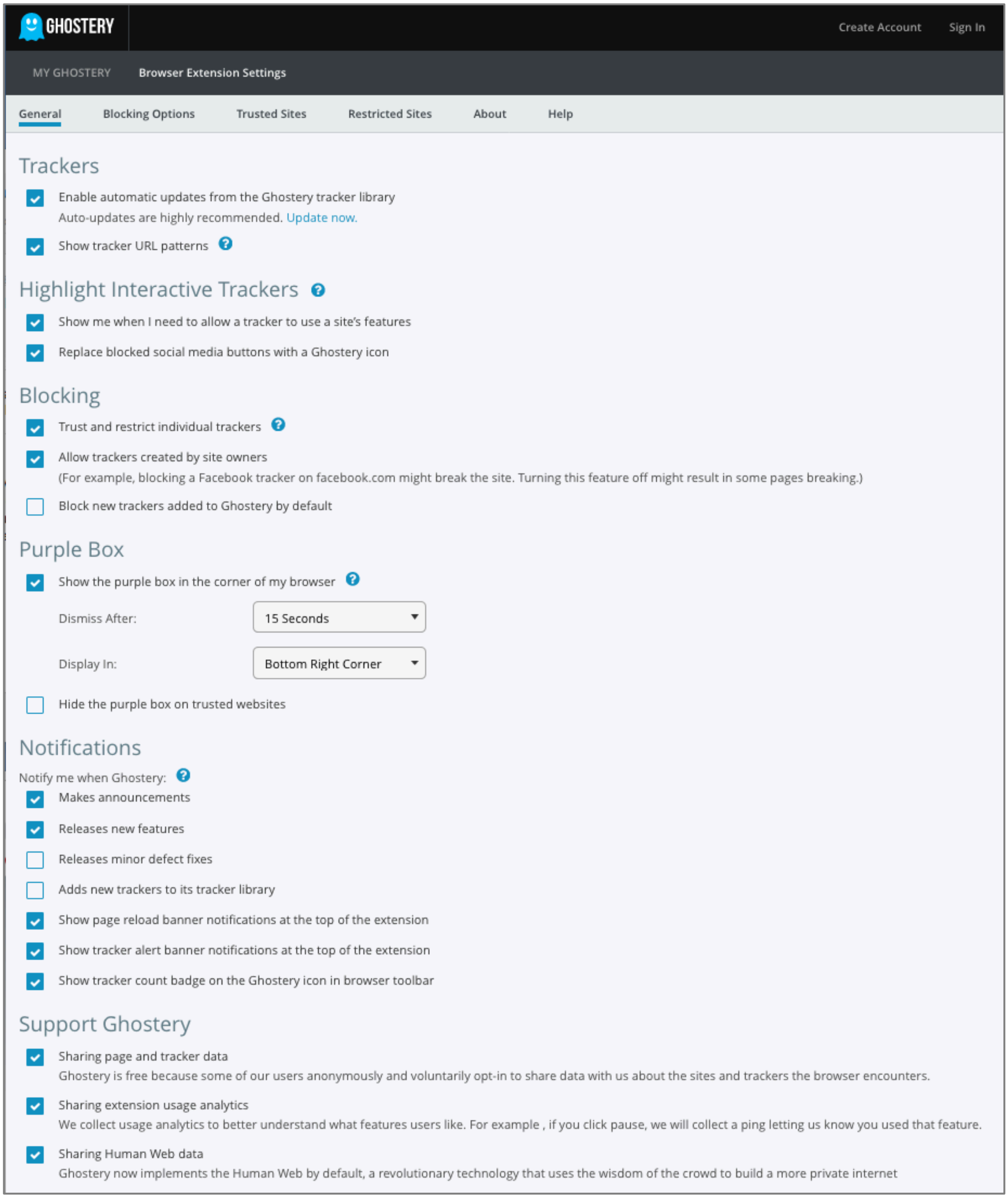
Essential
58 TRACKERS
Includes tag managers, privacy notices, and technologies that are critical to the functionality of a website. □

Audio/Video Player
55 TRACKERS
Enables websites to publish, distribute, and optimize video and audio content. □

Adult Advertising
22 TRACKERS
Delivers advertising technology designed specifically for adult content sites. □

Comments
10 TRACKERS
Enables comments sections for articles and product reviews. □

18. Select the *General* tab, and then configure to your taste.



Trackers

☑ Enable automatic updates from the Ghostery tracker library
Auto-updates are highly recommended. Update now.

☑ Show tracker URL patterns

Highlight Interactive Trackers

☑ Show me when I need to allow a tracker to use a site's features

☑ Replace blocked social media buttons with a Ghostery icon

Blocking

☑ Trust and restrict individual trackers

☑ Allow trackers created by site owners
(For example, blocking a Facebook tracker on facebook.com might break the site. Turning this feature off might result in some pages breaking.)

□ Block new trackers added to Ghostery by default

Purple Box

☑ Show the purple box in the corner of my browser

Dismiss After: 15 Seconds

Display In: Bottom Right Corner

□ Hide the purple box on trusted websites

Notifications

Notify me when Ghostery:

☑ Makes announcements

☑ Releases new features

□ Releases minor defect fixes

□ Adds new trackers to its tracker library

☑ Show page reload banner notifications at the top of the extension

☑ Show tracker alert banner notifications at the top of the extension

☑ Show tracker count badge on the Ghostery icon in browser toolbar

Support Ghostery

☑ Sharing page and tracker data
Ghostery is free because some of our users anonymously and voluntarily opt-in to share data with us about the sites and trackers the browser encounters.

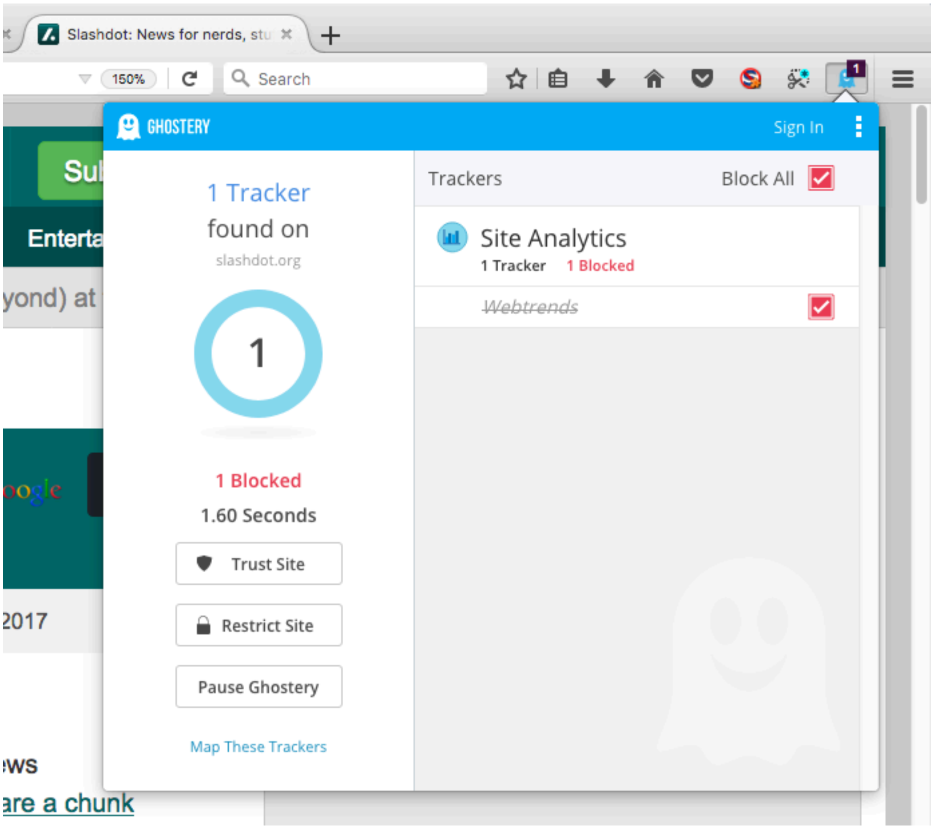
☑ Sharing extension usage analytics
We collect usage analytics to better understand what features users like. For example , if you click pause, we will collect a ping letting us know you used that feature.

☑ Sharing Human Web data
Ghostery now implements the Human Web by default, a revolutionary technology that uses the wisdom of the crowd to build a more private internet

19. Close the *Ghostery* page.

20. To test, visit *https://slashdot.com*.

21. Select the *Ghostery* icon in the toolbar. The Ghostery window will open, displaying any trackers on this page, and if they were blocked.



22. Close Firefox.

14.9 Adobe Flash and Java

Both Adobe Flash and Oracle Java are used by many websites to create a more animated or interactive web experience. Flash is no longer supported as a standalone System Preference and should be removed. Its functions are now built into the major web browsers, but will be removed when Adobe discontinues Flash support in 2020. The functions of both will soon be absorbed by HTML 5.

The power these products offer is a double-edged sword. They can also be used to take control of your computer. And often are. There is a vicious cat and mouse game played by hackers who have discovered how to bend Flash and Java to their wills, and Adobe and Oracle patching these vulnerabilities.

The result for users is they have a choice to make:

- Do not install Java, which renders some sites unusable.
- Install Java, and be vigilant with updates.
- Install Java, but don't be vigilant with updates, rendering your system vulnerable

I suspect if you are one who ops for the last option, you aren't taking this course.

Either of the other two options are legitimate strategies. Oracle has tried to make updates automatic, but we have found this process to be less than perfect. Many times, we have found systems with out of date versions, even with their preference settings on *Automatic Updates.*

Associated with the vulnerabilities caused by out of date Java, are malicious or compromised web pages that prompt the visitor to update Flash, Java, or some audio/video codec. In most cases, if you follow the links provided on the site all that gets downloaded is malware.

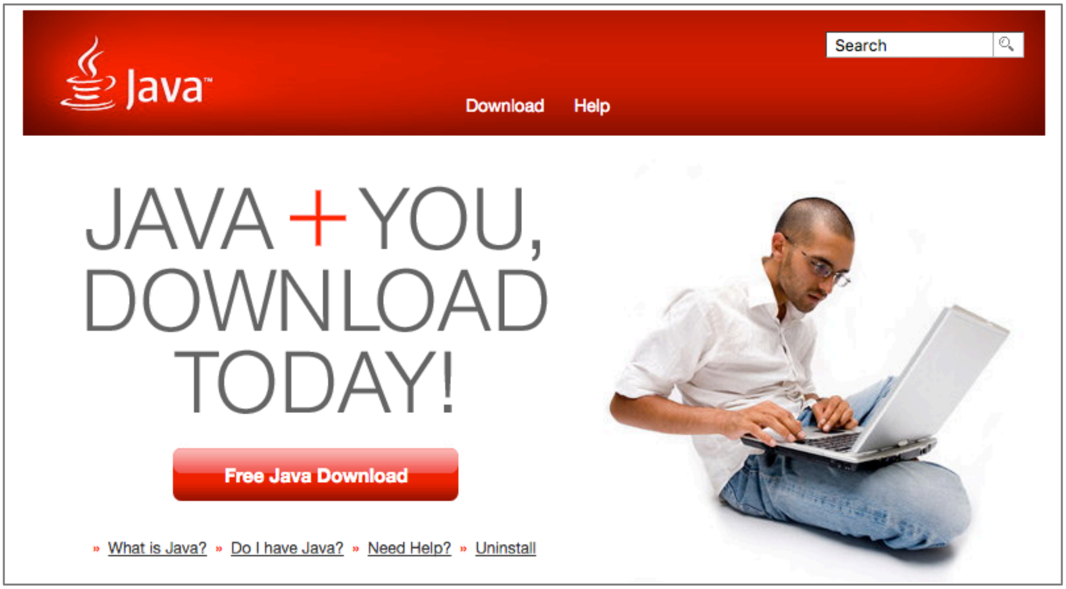
If a site prompts you do install software, visit the website of the recommended software and download from there, not from the requesting site.

14.9.1 Assignment: Configure Oracle Java for Automatic Updates

In this assignment, you install Java and configure it to automatically update.

Install Oracle Java.

1. Open *Apple* menu > *System Preferences.* If you see the Java icon, it is already installed. If so, skip to the next section *Configure Java for Auto-Updates.*
2. Open your browser to surf to *http://www.java.com/*.

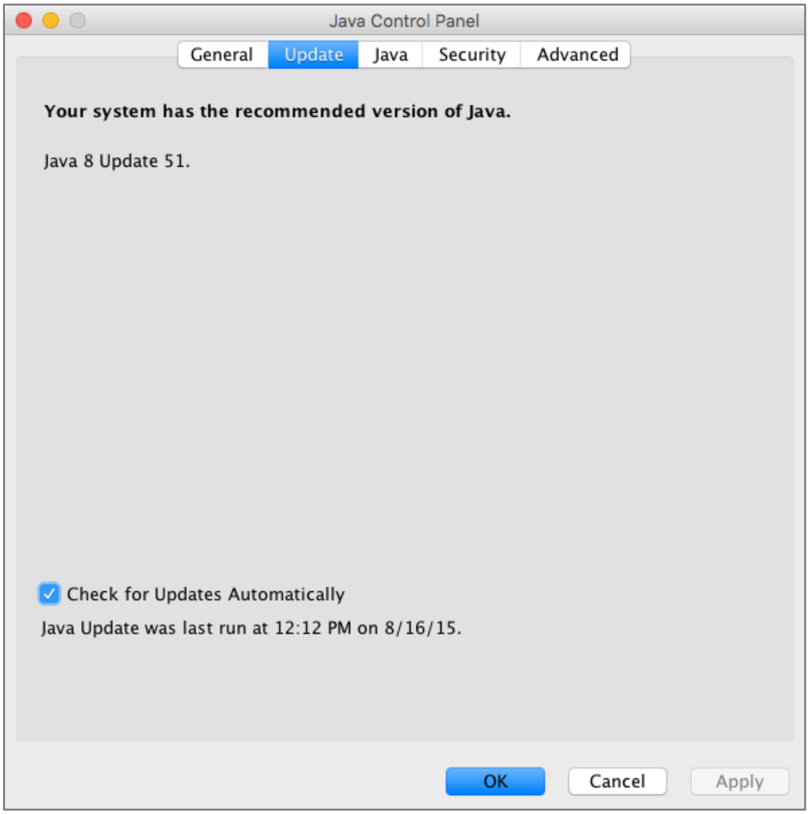

Java
Search
Download
Help
JAVA + YOU, DOWNLOAD TODAY!
Free Java Download
» What is Java? » Do I have Java? » Need Help? » Uninstall

3. Click the *Free Java Download* button.
4. Click the *Agree and Start Free Download* button.
5. Once the Java installer has downloaded, launch it, and then follow the on-screen instructions to complete installation.
6. When installation completes, restart your computer.

Configure Java for Auto-Updates.

7. Select *System Preferences* > *Java.*

8. Select the *Update* tab, and then enable the *Check for Updates Automatically* checkbox.



Your system has the recommended version of Java.

Java 8 Update 51.

☑ Check for Updates Automatically

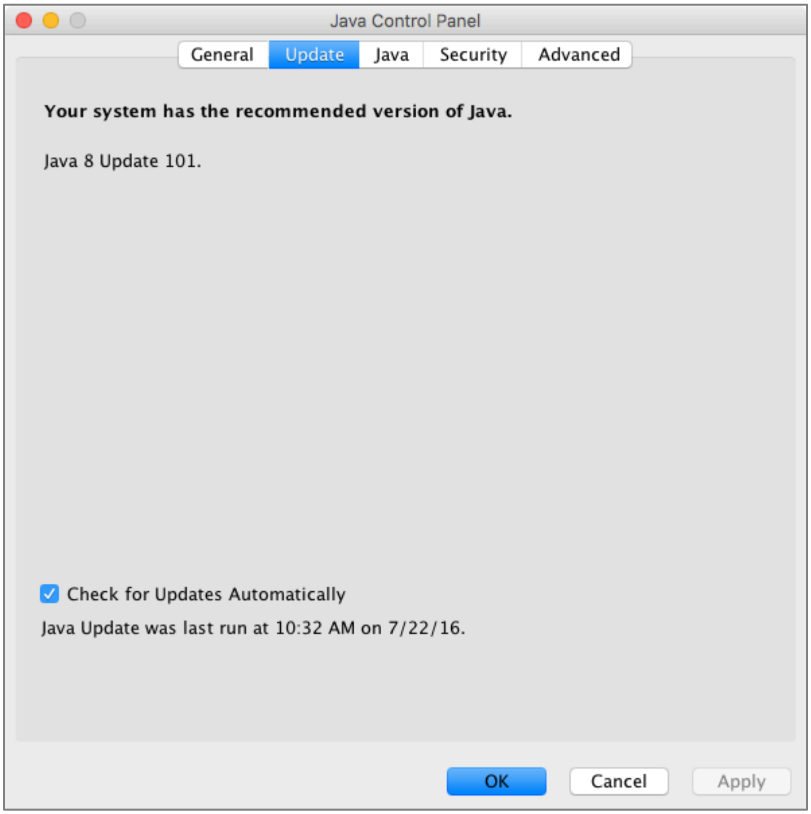
Java Update was last run at 12:12 PM on 8/16/15.

At this point, both your Flash and Java are up to date, and configured to automatically update. However, there is a decent chance that they will not do so. It is wise to perform a manual update check at least monthly.

Manually check for Java updates

9. Open *System Preferences > Java.*

10. Select the *Update* tab.



Your system has the recommended version of Java.

Java 8 Update 101.

☑ Check for Updates Automatically

Java Update was last run at 10:32 AM on 7/22/16.

11. If updates are available, select the *Update Now* button, and then follow the on-screen instructions to download and install.

14.10 Web Scams

Over the past couple of years, a new type of scam has become popular. Instead of directly compromising the user computer, web sites are either compromised, or are deliberately designed to be malicious.

When a user visits such a site, they may receive a pop-up window stating something to the effect of: *Your computer has been found to be infected with XX viruses. Please call Apple at XXX-XXX-XXXX to have this infection removed.*

Upon calling the provided toll-free phone number (which, of course, is not Apple, but that of the scammer), with your permission, they will install remote control software. After looking around your computer, they will assure they can remove the malware for only $$$.

There are two problems here. First, they have installed remote control software that allows the criminal access any time they wish. This gives them access to your usernames, passwords, banking, and other information. The second is that they now have your credit card information.

14.10.1 Recovering From A Web Scam

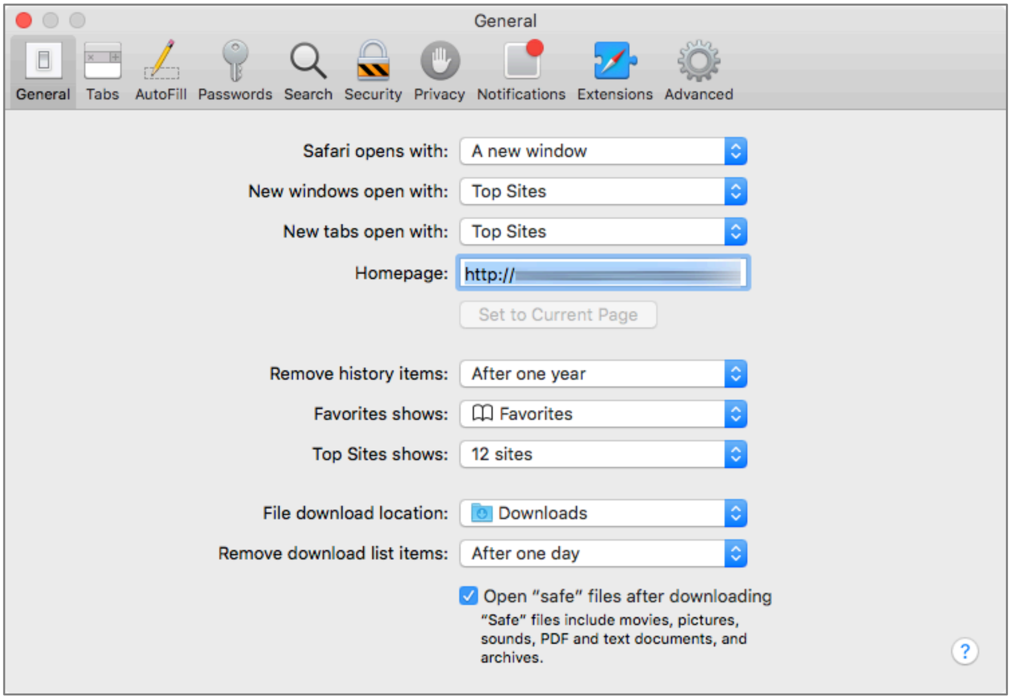
What to do if this happens to you?

In this assignment, you examine Safari for possible modifications.

1. Don't call!

In most cases, the malicious website has modified your web browser preferences to make the malicious page your home page.

2. Open your browser *preferences* (in this example, Safari) > *General.* If the *Homepage* field is not what you have set, delete the entry.



Safari opens with: A new window

New windows open with: Top Sites

New tabs open with: Top Sites

Homepage: http://[redacted]

Set to Current Page

Remove history items: After one year

Favorites shows: Favorites

Top Sites shows: 12 sites

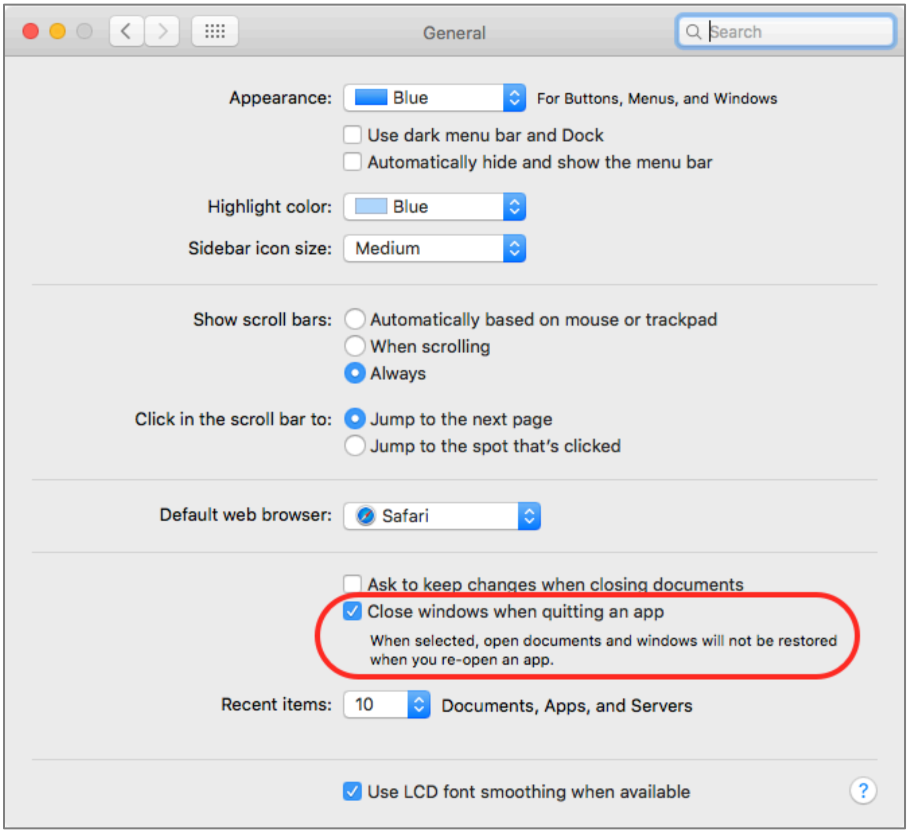
File download location: Downloads

Remove download list items: After one day

☑ Open "safe" files after downloading
"Safe" files include movies, pictures, sounds, PDF and text documents, and archives.

3. Malicious attacks on a browser often will block access to the browser preferences. If you are not able to access your browser preferences to delete

the homepage setting, open *System Preferences* > *General*, and then enable *Close windows when quitting an app.*



Appearance: Blue — For Buttons, Menus, and Windows

□ Use dark menu bar and Dock

□ Automatically hide and show the menu bar

Highlight color: Blue

Sidebar icon size: Medium

Show scroll bars:
○ Automatically based on mouse or trackpad
○ When scrolling
● Always

Click in the scroll bar to:
● Jump to the next page
○ Jump to the spot that's clicked

Default web browser: Safari

□ Ask to keep changes when closing documents

☑ Close windows when quitting an app

When selected, open documents and windows will not be restored when you re-open an app.

Recent items: 10 Documents, Apps, and Servers

☑ Use LCD font smoothing when available

4. Quit Safari.
5. Open Safari to test. You should no longer have the malicious page open.

Done!

14.11 Tor

Tor[10] is a technology developed by the US Department of the Navy that enables anonymous web browsing. It has long since been released to the open source community for the public to use in the form of the *Tor Browser*. Many people within the security community are strong supporters of Tor, including Edward Snowden. Entire books have been written on just Tor. I'm not so sadistic as to subject you to that. What we are going to do is cut to the core of Tor, and learn the basics of how to surf the web anonymously.

The advantages of Tor include:

- Strong anonymity for all activity on the Internet.
- Can be used with Tails[11] which is a bootable, self-contained, flash drive that can run on most Windows, Linux, and Apple computers that leaves no trace behind.
- The bootable Tails flash drive can be immediately disconnected from the host computer, causing the computer to erase memory of all trace of your session, and reboot.

The disadvantages of Tor include:

- It was developed by the US Department of the Navy. It is possible there are back doors only the government knows about.
- The US government has been forthright about having its own Tor relays in place, which enable it to monitor online activity. Not a big deal if you only wish to be anonymous to criminals. It is a big deal if you wish to be anonymous while performing black-market deals for my Aunt Rose's raisin Noodle Koogle recipe.

These features make Tor ideal for those in oppressed countries, journalists working undercover, and anyone who may need to use someone else's computer and leave no trace behind.

[10] *http://en.wikipedia.org/wiki/Tor_(anonymity_network)*

[11] *https://tails.boum.org*

Tor works by encrypting your packets as they leave your computer, routing the packets to a Tor relay computer hosted by thousands of volunteers on their own systems, many of which are co-located at ISPs. The relay knows where the packet came from, and the next relay the packet is handed to, but that is all. The user computer automatically configures encrypted connections through the relays. Packets will pass through several relays before being delivered to the intended destination. Tor will use the same relays for around 10 minutes, and then different relays will be randomly selected to create the next path for 10 minutes.

Alas, there is no free lunch. The encryption process and the relay process combine to create *latency*, which mean a delay in processing. Most users will experience around a four-fold performance degradation. So, if accessing a web page without Tor normally takes 3 seconds, it may take 12 seconds with Tor.

Even though Tor does as good a job as anything to keep you anonymous on the Internet, you must take precautions to protect your identity. These steps include:

- Don't enable JavaScript when using Tor. This has been used to track users within the Tor network.
- Don't reveal your name or other personal information in web forms.
- Don't customize the Tails boot flash drive. This will create a unique digital fingerprint that can be used to identify you.
- Connect to sites that use HTTPS so your communications are encrypted point to point.

For many security-conscious users, Tor becomes their only tool for defense. However, Tor by itself is at best a partial solution. It can protect your anonymity while surfing the web. At the very least, this still leaves email and messaging to be secured. A bigger issue is what to do when you need to use a computer and leave no trace behind on that system. This is where *Tails* comes into play.

Tails is a Linux Debian fork designed with two primary purposes in mind:

- Provide a highly secure operating system in a format that can be booted from either DVD or thumb drive on almost any PC or Apple computer, and
- Include the tools and applications necessary to provide a secure, anonymous Internet experience

What this means is that you can create a thumb drive that has an operating system capable of booting almost any computer, whereby you can then run Tor for secure anonymous Internet activity, send and receive email that is securely encrypted with GPG/PGP, and message with others in complete privacy. Then, when you remove the Tails thumb drive, there is absolutely no record of your activity on either the computer *or* the thumb drive!

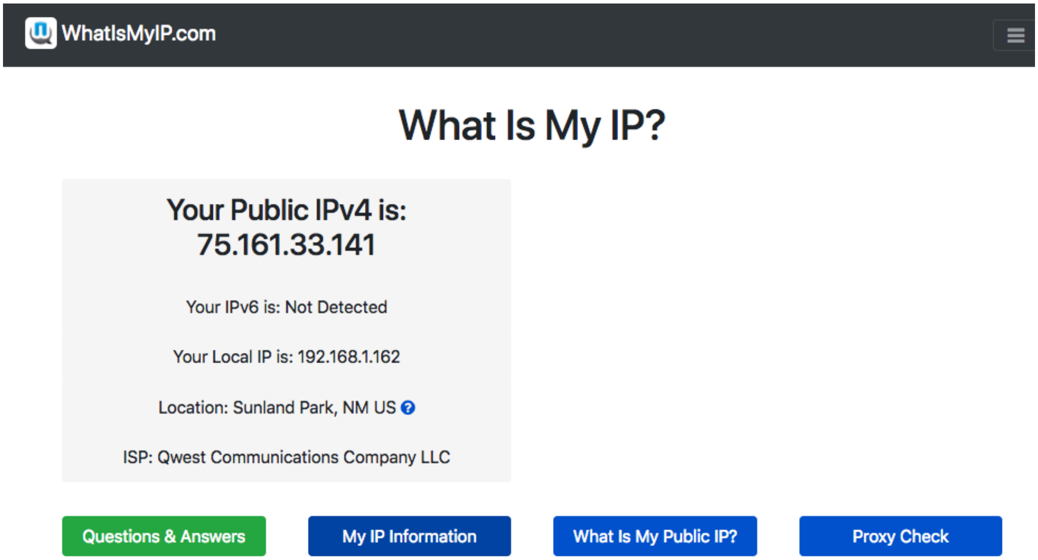
For those of you chomping at the bit to just use Tor, we will start there. When your curiosity has been satisfied, please take the next step to learn Tails[12].

14.11.1 Assignment: Install Tor for Anonymous Internet Browsing

Tor is a stripped down, simplified web browser, designed to provide an encrypted, anonymous browsing experience.

In this assignment, you download and install Tor.

1. As a first step, we need to know our public IP address. This information will be used a few steps away to verify Tor has hidden our address. Open a web browser to *https://whatismyip.com*. Write down *Your IP*.



What Is My IP?

Your Public IPv4 is:
75.161.33.141

Your IPv6 is: Not Detected

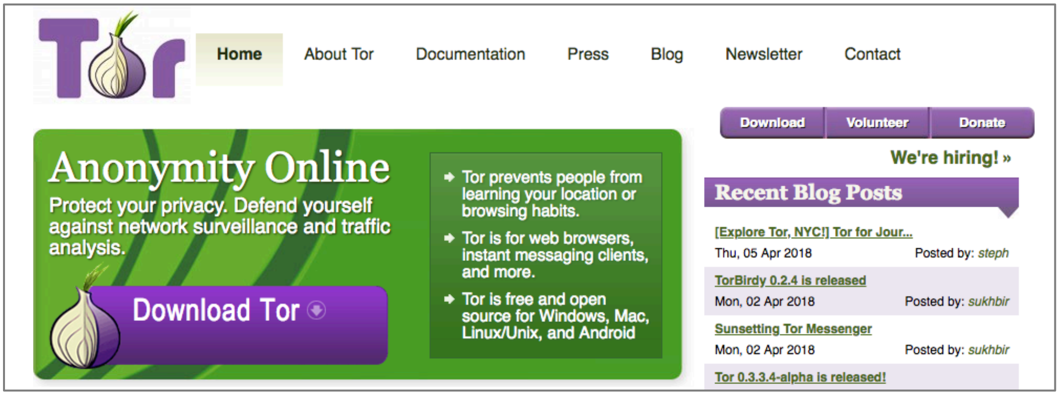
Your Local IP is: 192.168.1.162

Location: Sunland Park, NM US

ISP: Qwest Communications Company LLC

[12] https://tails.boum.org

2. Open a web browser and then go to *https://www.torproject.org*. Select the *Download Tor* button.



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Recent Blog Posts

[Explore Tor, NYC!] Tor for Jour...
Thu, 05 Apr 2018 Posted by: *steph*

TorBirdy 0.2.4 is released
Mon, 02 Apr 2018 Posted by: *sukhbir*

Sunsetting Tor Messenger
Mon, 02 Apr 2018 Posted by: *sukhbir*

Tor 0.3.3.4-alpha is released!

3. Select the *Download Tor Browser* button. The Tor installer will begin to download.

4. While the download is in progress, scroll down the page to read all the other steps that one must take to ensure your privacy is maintained. These include:

   - **Use the Tor Browser.** If you are concerned about protecting your privacy and security, do not use other browsers.

   - **Don't torrent over Tor.** If you wish to file-share via torrent, don't use Tor. It is painfully slow, it slows down others using the Tor network, and in many cases, torrent software bypasses all the security and anonymity precautions built into Tor.

   - **Don't enable or install browser plugins in Tor.** Tor is designed to protect your security and anonymity. Many innocuous-looking plugins break that security.

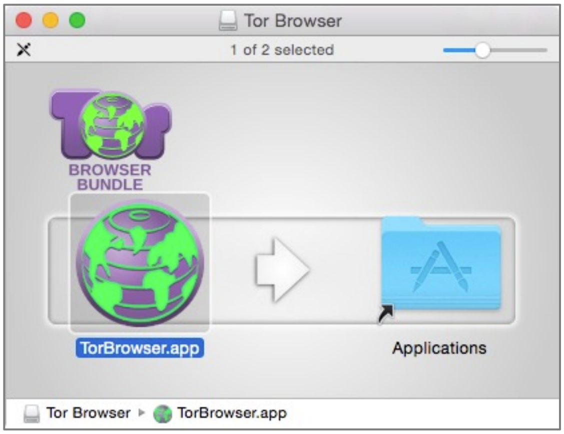
   - **Use HTTPS versions of websites.** Tor has *HTTPS Everywhere* built in (more on HTTPS Everywhere later in this book.) It will force a secure connection if a website has an option for https. This will enable a point-to-point encryption between your computer and the web server.

   - **Don't open documents downloaded through Tor while online.** Many documents–particularly .doc, .xls, .ppt, and .pdf–contain links or resources that will force a download when the document is opened. If they are opened while Tor is open, they will reveal your true IP address and you will lose your anonymity and security. If you are concerned about these issues, we strongly recommend that you instead:

  - **Open the documents on a computer fully disconnected from the Internet**. This prevents any malicious files from "phoning home" or infecting your computer.
  - **Install a Virtual Machine (VM) such as Parallels, Fusion, or VirtualBox, configured with no network connection, and open documents within the VM**. This is an alternate way to prevent malicious files from phoning home or infecting your computer.
  - **Or use Tor while within Tails**. This is an alternative way to prevent malicious files from phoning home or infecting your computer.

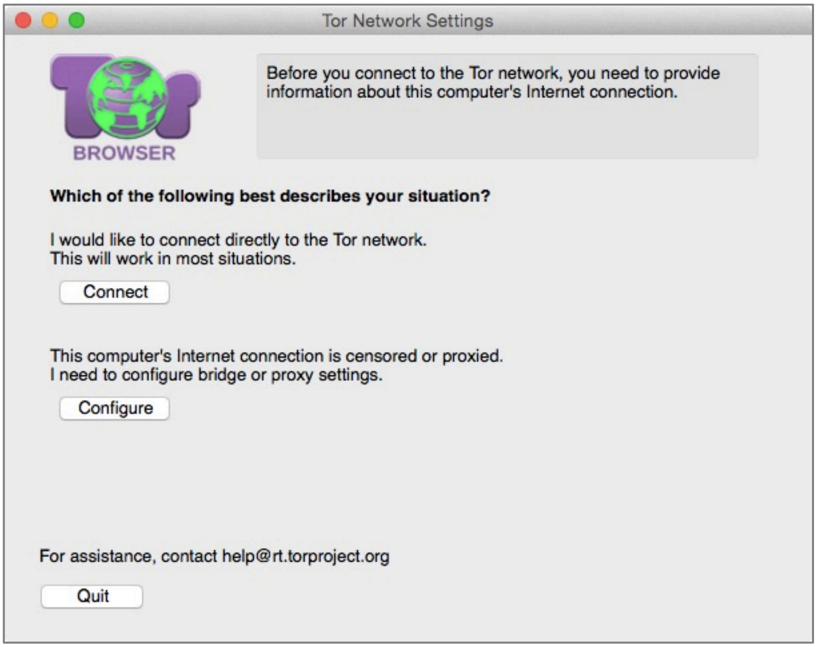
- **Use bridges and/or find company.** Tor cannot prevent someone from looking at your Internet traffic to discover you are using Tor. If this is a concern for you, reduce the risk by configuring Tor to use a *Tor Bridge relay* instead of a direct connection to the Tor network. Another option is to have many other users running Tor on the same network. In this way, your use of Tor is hidden.

5. Locate the Tor installer, and then double-click to open. It will mount and open a disk image onto the Desktop.
6. Drag the *TorBrowser.app* into your *Applications* folder.



7. Locate the *TorBrowser* in your Applications folder, and then double-click to open it. The *Tor Network Settings* window appears. Select how you would like to connect to the Tor Network

   - *I would like to connect directly to the Tor network.* This will work in most situations. This option provides a faster Internet experience with no additional configuration. The possible downside is that a network administrator or your ISP can see that you are using the Tor Network.
   - *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings.* This option provides a more secure and anonymous Internet experience as a network administrator or ISP is unable to see you using the Tor Network. The downside is a slower Internet experience, and some additional configuration.



Tor Network Settings

Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

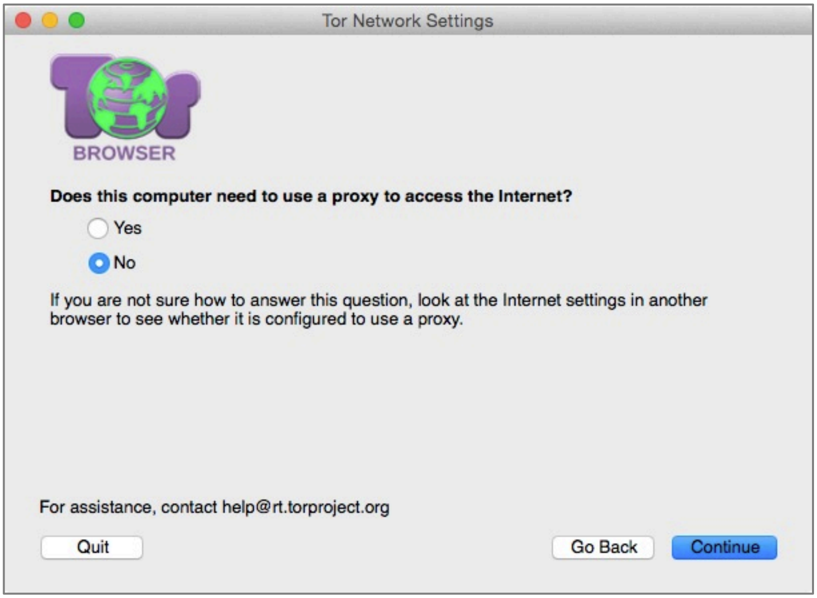
I would like to connect directly to the Tor network.
This will work in most situations.

This computer's Internet connection is censored or proxied.
I need to configure bridge or proxy settings.

For assistance, contact help@rt.torproject.org

8. If you selected *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings*, go to the next step. If you *selected I would like to connect directly to the Tor network*, skip to step 14.

9. If you elected to use a *Tor bridge relay*, the following window appears. If your network requires a proxy to access the Internet, go to the next step and select *Continue*. Otherwise, select *No,* select the *Continue* button, and skip to step 12.



Does this computer need to use a proxy to access the Internet?

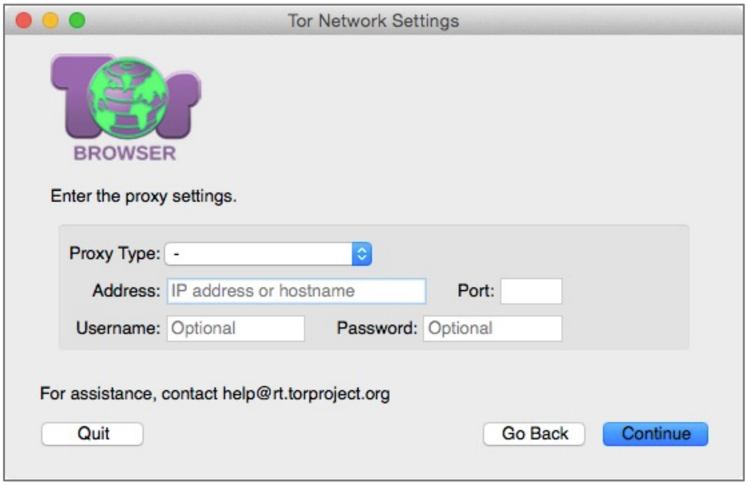
○ Yes

● No

If you are not sure how to answer this question, look at the Internet settings in another browser to see whether it is configured to use a proxy.

For assistance, contact help@rt.torproject.org

10. If you selected *Yes* to *Does this computer need to use a proxy to access the Internet* you will now see the Enter the Proxy settings window.



Enter the proxy settings.

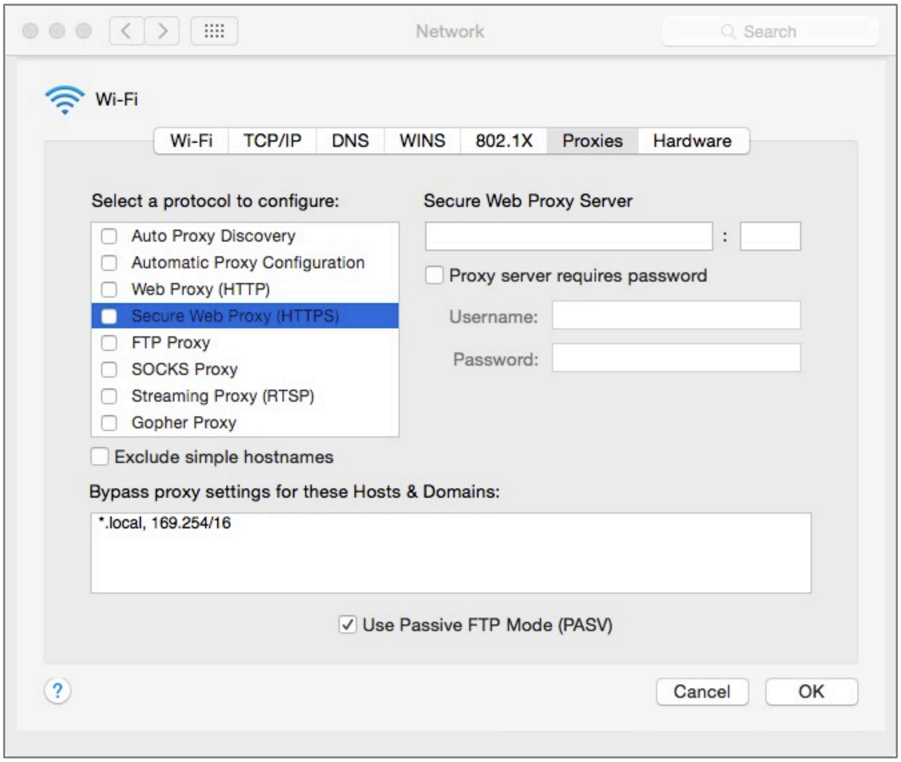
Proxy Type: -

Address: IP address or hostname Port:

Username: Optional Password: Optional

For assistance, contact help@rt.torproject.org

11. These will be the same settings your computer requires normally, and if used, will be found in *System Preferences > Network > Advanced > Proxies* tab. Copy your settings from this pane into the Tor window, and then select the *Continue* button. If your ISP blocks or otherwise censor's connections to the Tor network, go to the next step to create a Tor bridge relay. If they do not, skip to step 14 to start using Tor.



Select a protocol to configure:

□ Auto Proxy Discovery
□ Automatic Proxy Configuration
□ Web Proxy (HTTP)
□ Secure Web Proxy (HTTPS)
□ FTP Proxy
□ SOCKS Proxy
□ Streaming Proxy (RTSP)
□ Gopher Proxy

Secure Web Proxy Server
:

□ Proxy server requires password

Username:

Password:

□ Exclude simple hostnames

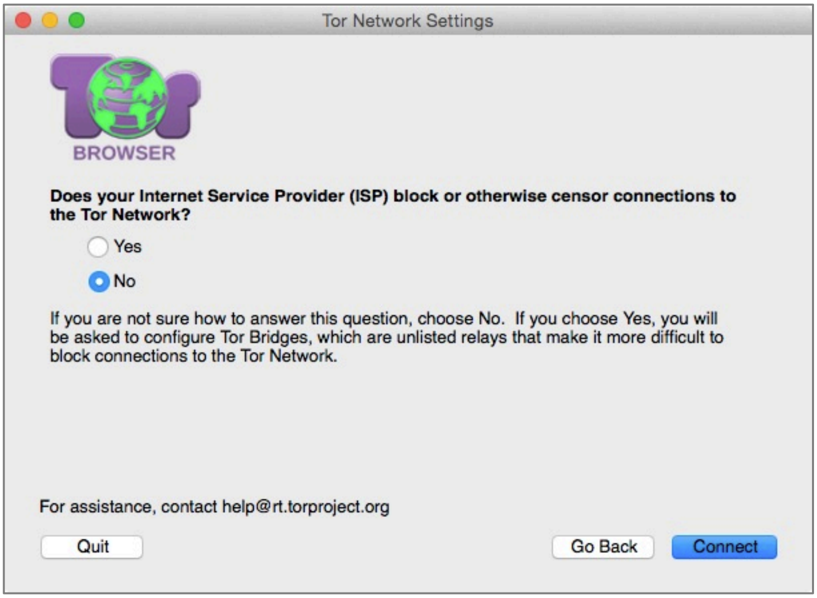
Bypass proxy settings for these Hosts & Domains:

*.local, 169.254/16

☑ Use Passive FTP Mode (PASV)

12. At the *Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network* window, for the overwhelming majority of users the answer is *No,* and then select the *Connect* button, and then skip to

step 14. If your answer is *Yes,* select the *Yes* option, select the *Continue* button, and go to the next step.



Tor Network Settings

Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network?

○ Yes

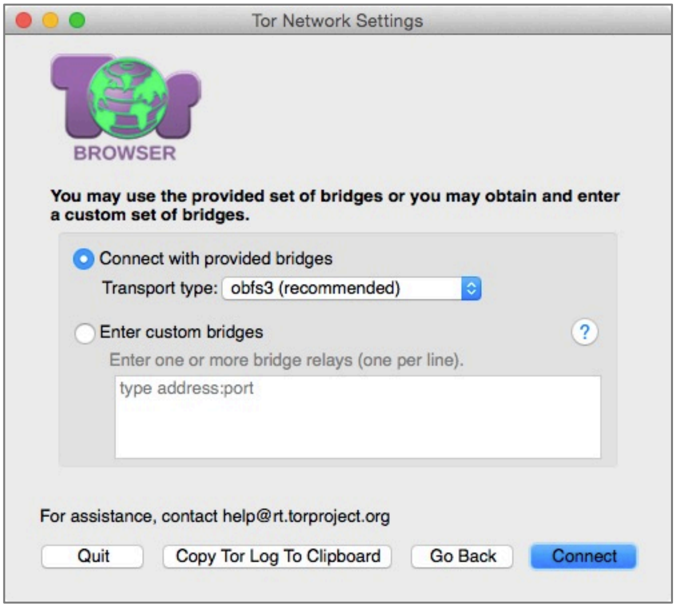
● No

If you are not sure how to answer this question, choose No. If you choose Yes, you will be asked to configure Tor Bridges, which are unlisted relays that make it more difficult to block connections to the Tor Network.

For assistance, contact help@rt.torproject.org

13. If you selected Yes to the *Does your ISP block or otherwise censor connections to the Tor* Network window, you now see the You may use the provided set of bridges or you may obtain and enter a customer set of bridges window. Select

Connect with provided bridges, Transport type obsf3 (recommended), and then select the *Connect* button.



You may use the provided set of bridges or you may obtain and enter a custom set of bridges.

● Connect with provided bridges

Transport type: obfs3 (recommended)

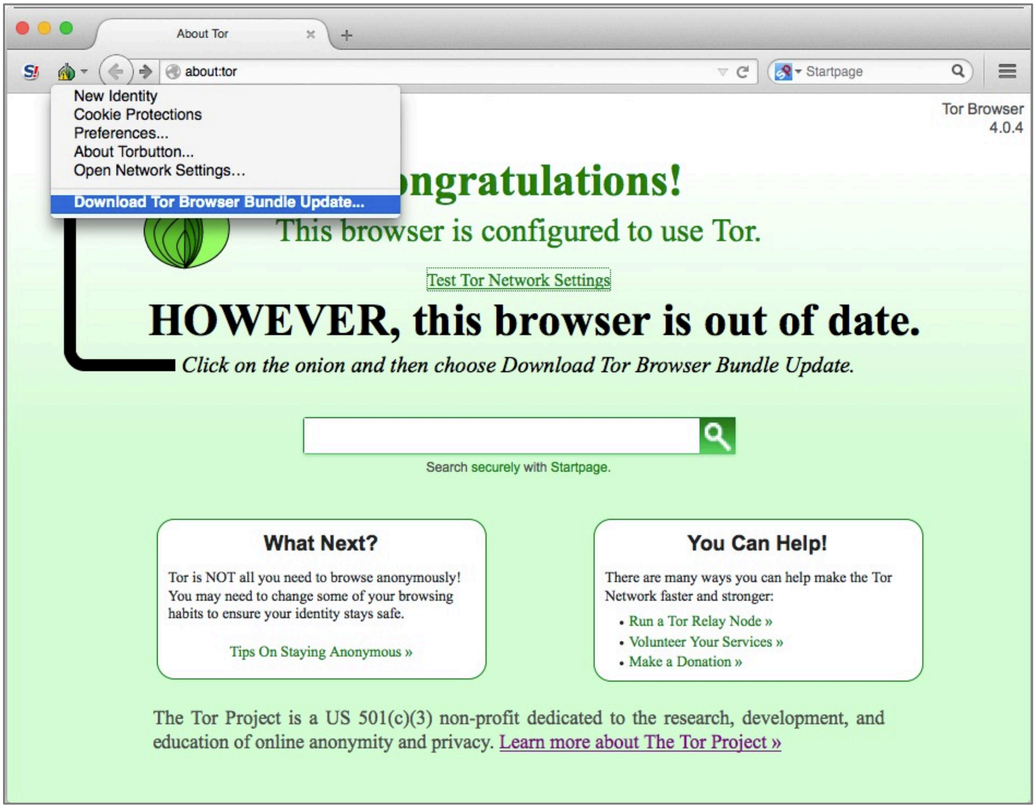
○ Enter custom bridges

Enter one or more bridge relays (one per line).

type address:port

For assistance, contact help@rt.torproject.org

14. The Tor Browser updates often. If your copy is out of date, you will be welcomed by a message asking you to update. Follow the instructions, clicking on the *onion* icon > *Download Tor Browser Bundle Update…*to update. Once the download is complete, Quit Tor Browser, and then replace it with the new version. Otherwise, if you are up to date, skip to the next step.



ngratulations!

This browser is configured to use Tor.

Test Tor Network Settings

HOWEVER, this browser is out of date.

Click on the onion and then choose Download Tor Browser Bundle Update.

Search securely with Startpage.

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 »

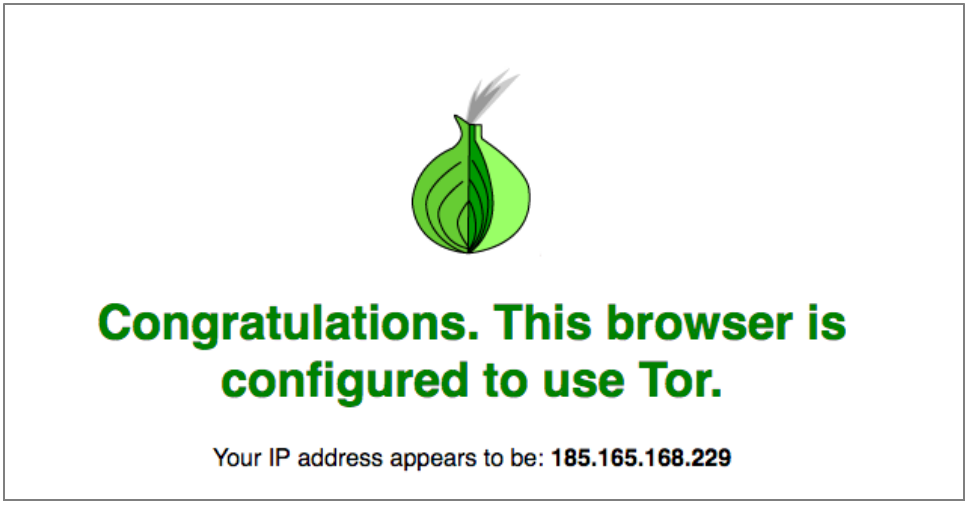
You Can Help!

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 »

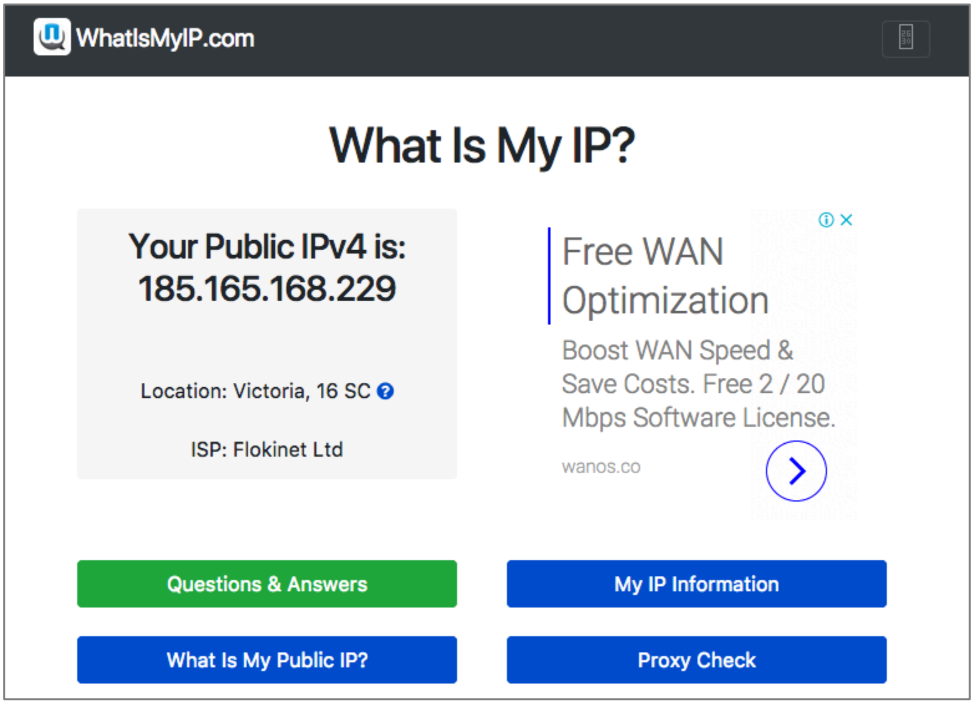
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

15. It is vital to test your connection to verify your IP address is hidden/changed. While in Tor, go to *https://check.torproject.org*. You can also return to *https://whatismyip.com* as well.



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **185.165.168.229**



What Is My IP?

Your Public IPv4 is:
185.165.168.229

Location: Victoria, 16 SC

ISP: Flokinet Ltd

Free WAN Optimization

Boost WAN Speed & Save Costs. Free 2 / 20 Mbps Software License.

wanos.co

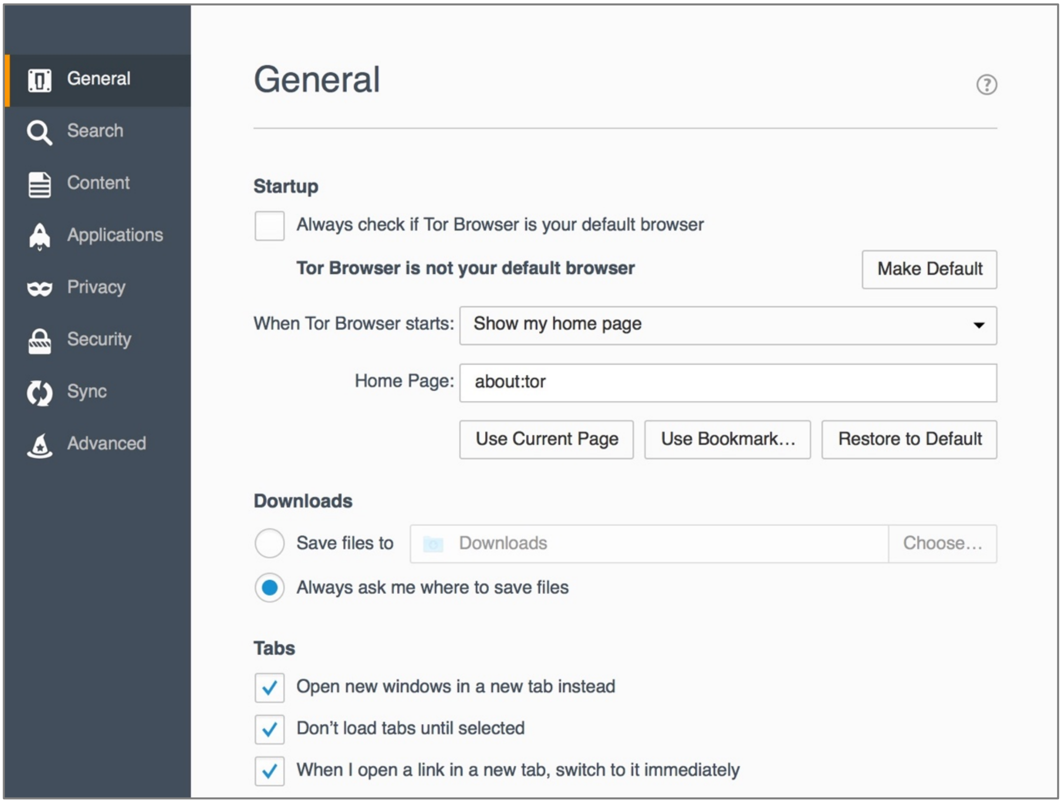
Wahoo! You are now on Tor, completely anonymous and encrypted on the Internet. Next step is to configure Tor.

5.1.1 Assignment: Configure Tor Preferences

One of the first things one should do when launching an application for the first time is to configure its preferences. No different for Tor.

In this assignment, you configure Tor preferences.

1. Open TorBrowser, and then select the *3 horizontal line* menu (top right) > *Preferences* > *General* tab. This pane may be configured to taste.



General

Startup

□ Always check if Tor Browser is your default browser

Tor Browser is not your default browser

When Tor Browser starts: Show my home page

Home Page: about:tor

Downloads

○ Save files to Downloads

● Always ask me where to save files

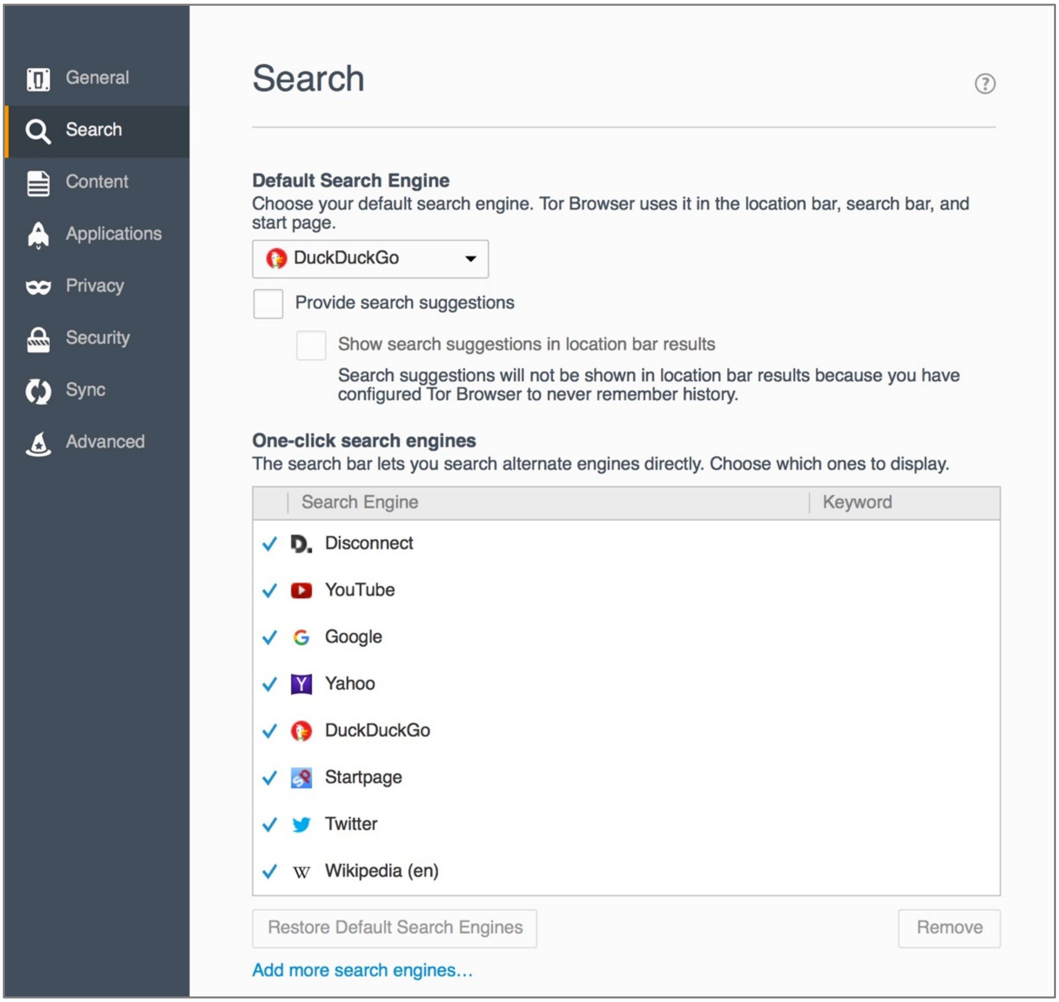
Tabs

☑ Open new windows in a new tab instead

☑ Don't load tabs until selected

☑ When I open a link in a new tab, switch to it immediately

2. Select the *Search* tab.



Search

Default Search Engine

Choose your default search engine. Tor Browser uses it in the location bar, search bar, and start page.

DuckDuckGo

□ Provide search suggestions

□ Show search suggestions in location bar results

Search suggestions will not be shown in location bar results because you have configured Tor Browser to never remember history.

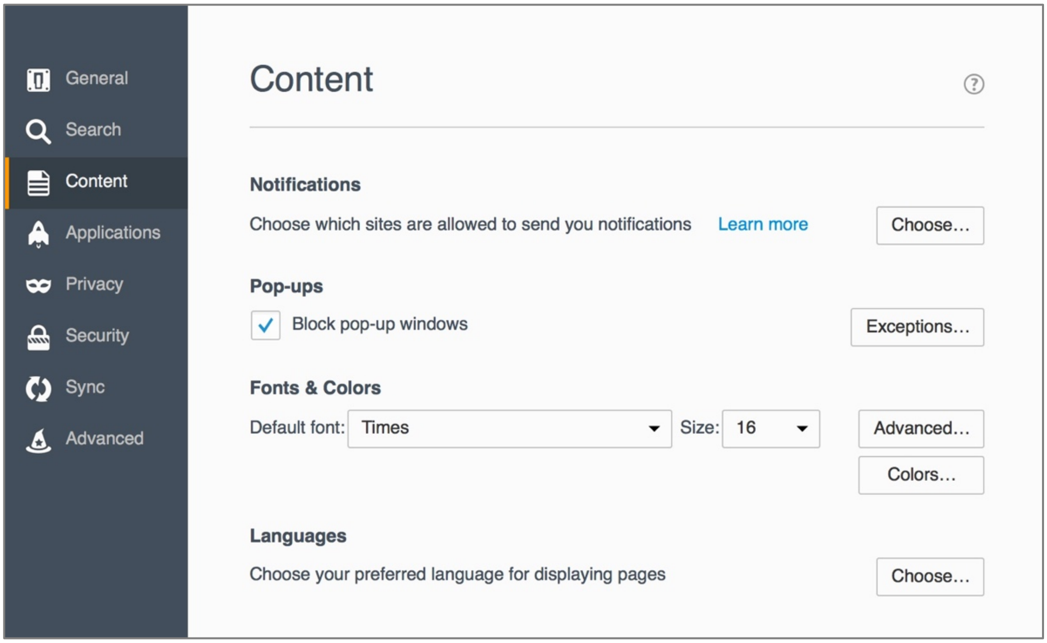
One-click search engines

The search bar lets you search alternate engines directly. Choose which ones to display.

	Search Engine	Keyword
✓	Disconnect	
✓	YouTube	
✓	Google	
✓	Yahoo	
✓	DuckDuckGo	
✓	Startpage	
✓	Twitter	
✓	Wikipedia (en)	

- For *Default Search Engine,* select *DuckDuckGo.*
- Other settings may be configured to your taste.

3. Select the *Content* tab. Configure to your taste.



Content

Notifications

Choose which sites are allowed to send you notifications Learn more

Pop-ups

☑ Block pop-up windows

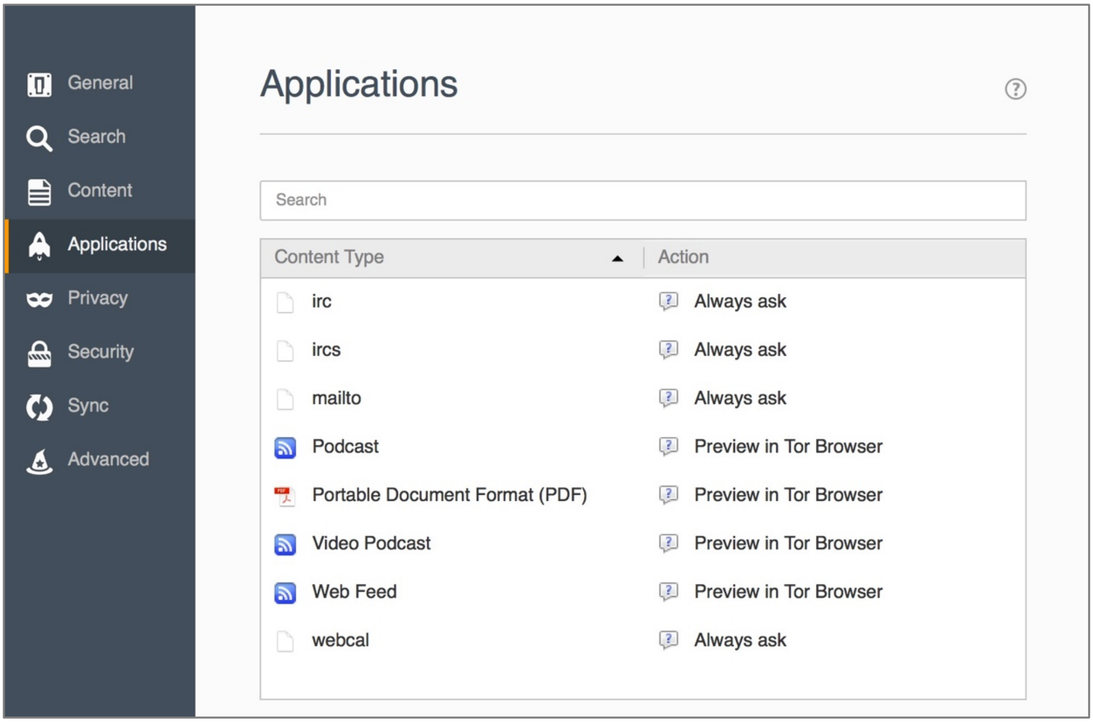
Fonts & Colors

Default font: Times Size: 16

Languages

Choose your preferred language for displaying pages

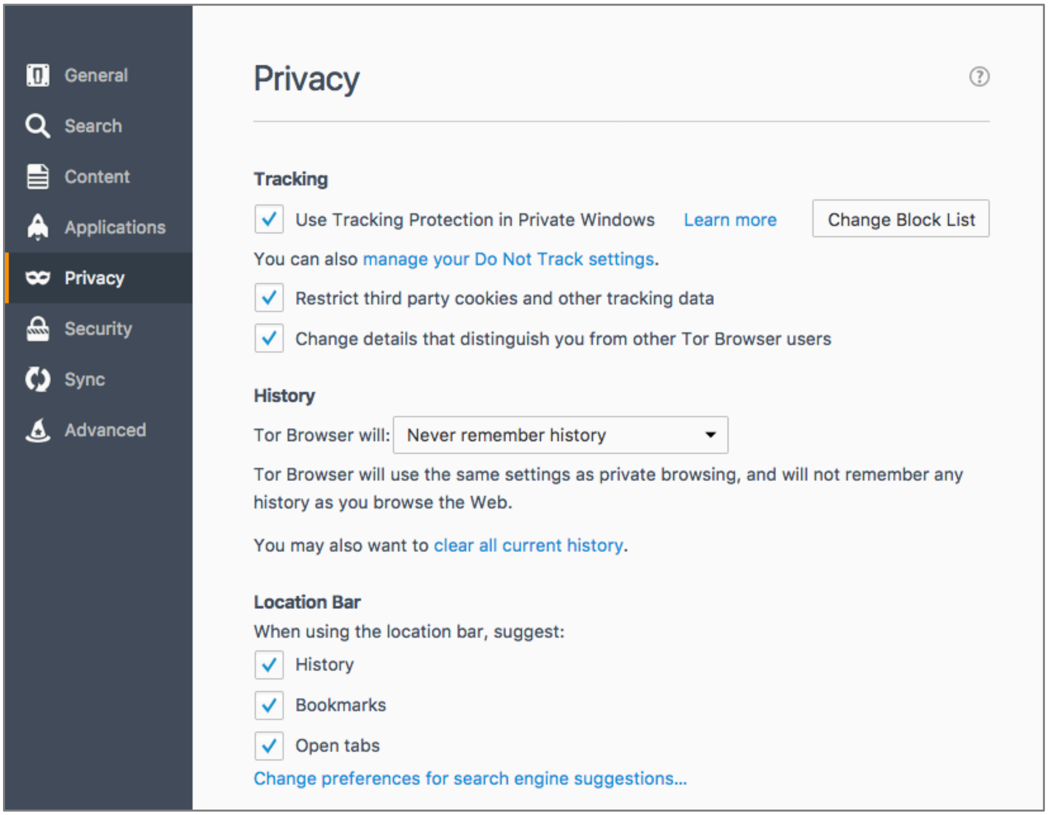
4. Select the *Applications* tab. Configure to your taste.



Applications

Content Type	Action
irc	Always ask
ircs	Always ask
mailto	Always ask
Podcast	Preview in Tor Browser
Portable Document Format (PDF)	Preview in Tor Browser
Video Podcast	Preview in Tor Browser
Web Feed	Preview in Tor Browser
webcal	Always ask

5. Select the *Privacy* tab.



Privacy

Tracking

☑ Use Tracking Protection in Private Windows Learn more Change Block List

You can also manage your Do Not Track settings.

☑ Restrict third party cookies and other tracking data

☑ Change details that distinguish you from other Tor Browser users

History

Tor Browser will: Never remember history

Tor Browser will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

Location Bar

When using the location bar, suggest:

☑ History

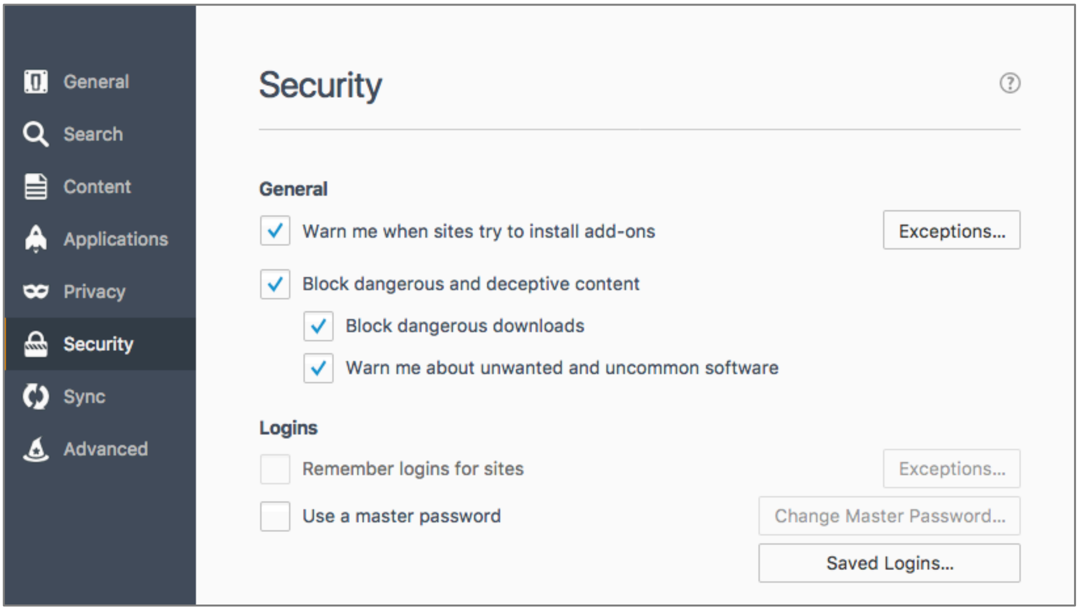
☑ Bookmarks

☑ Open tabs

Change preferences for search engine suggestions...

- Enable *Tracking > Use Tracking Protection in Private Windows*
- Enable *History > Tor Browser will: > Never remember history*
- *Location Bar* may be configured to your taste.

6. Select the *Security* tab.



Security

General

☑ Warn me when sites try to install add-ons

☑ Block dangerous and deceptive content

☑ Block dangerous downloads

☑ Warn me about unwanted and uncommon software

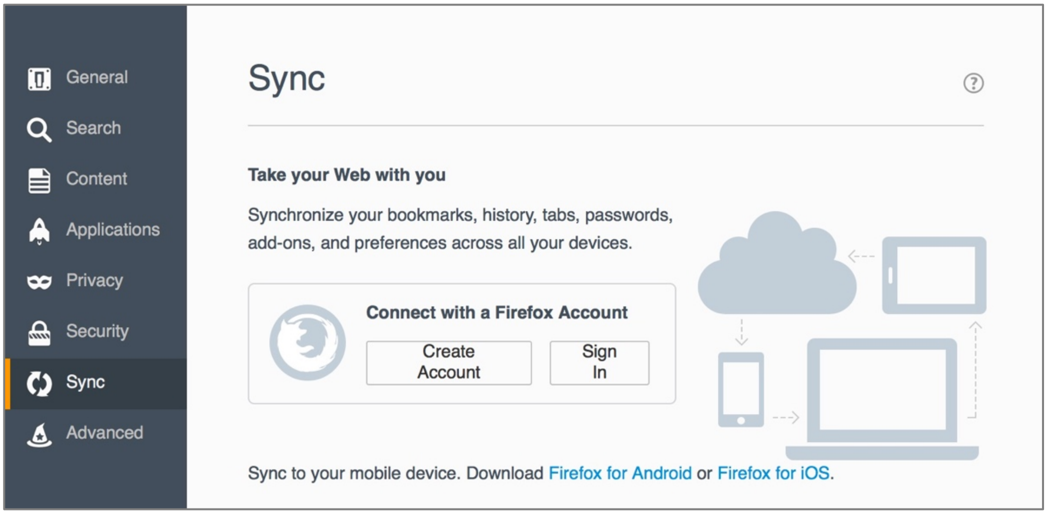
Logins

□ Remember logins for sites

□ Use a master password

- Enable *General* > *Warn me when sites try to install add-ons.*
- Enable *General* > *Block reported attack sites.*
- Enable *General* > *Block reported web forgeries.*
- Configure other settings to your taste.

7. Select the *Sync* tab.



Sync

Take your Web with you

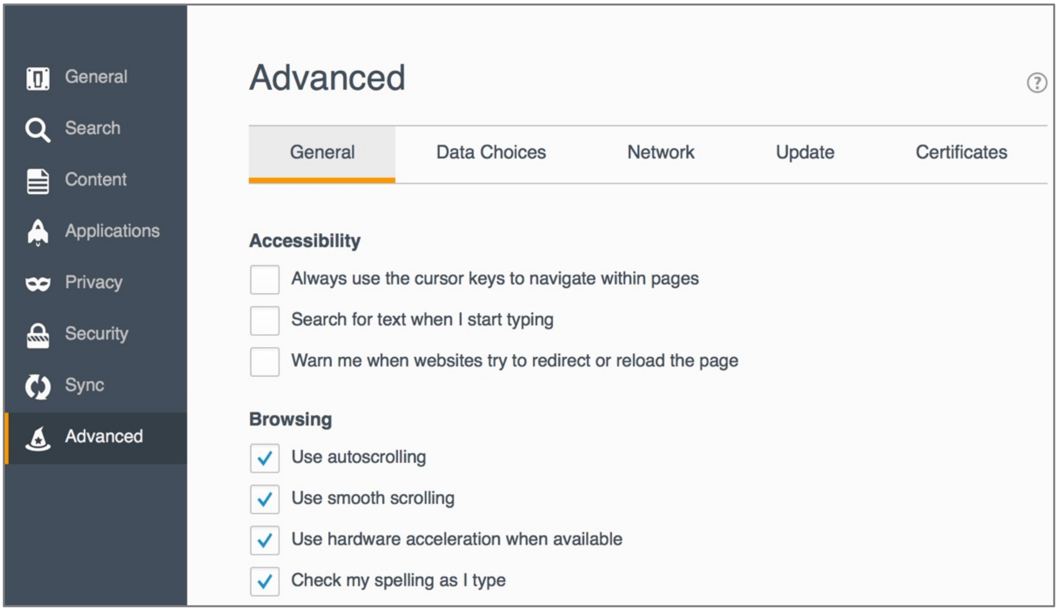
Synchronize your bookmarks, history, tabs, passwords, add-ons, and preferences across all your devices.

Connect with a Firefox Account

Sync to your mobile device. Download Firefox for Android or Firefox for iOS.

- Configure to your taste.

8. Select the *Advanced* tab, and then select the *General* tab.



Advanced

Accessibility

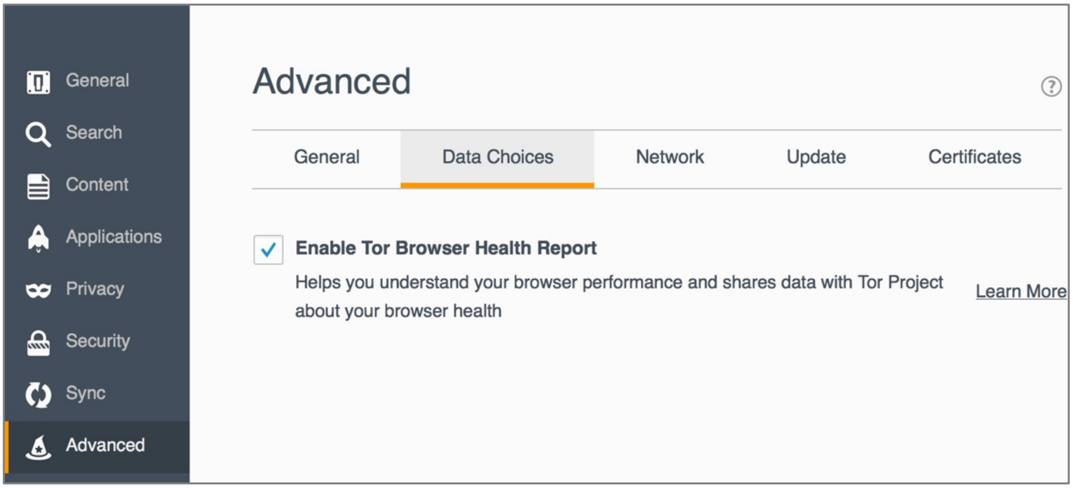
□ Always use the cursor keys to navigate within pages
□ Search for text when I start typing
□ Warn me when websites try to redirect or reload the page

Browsing

☑ Use autoscrolling
☑ Use smooth scrolling
☑ Use hardware acceleration when available
☑ Check my spelling as I type

- Configure to your taste.

9. Select the *Data Choices* tab, and then enable *Enable Tor Browser Health Report*.



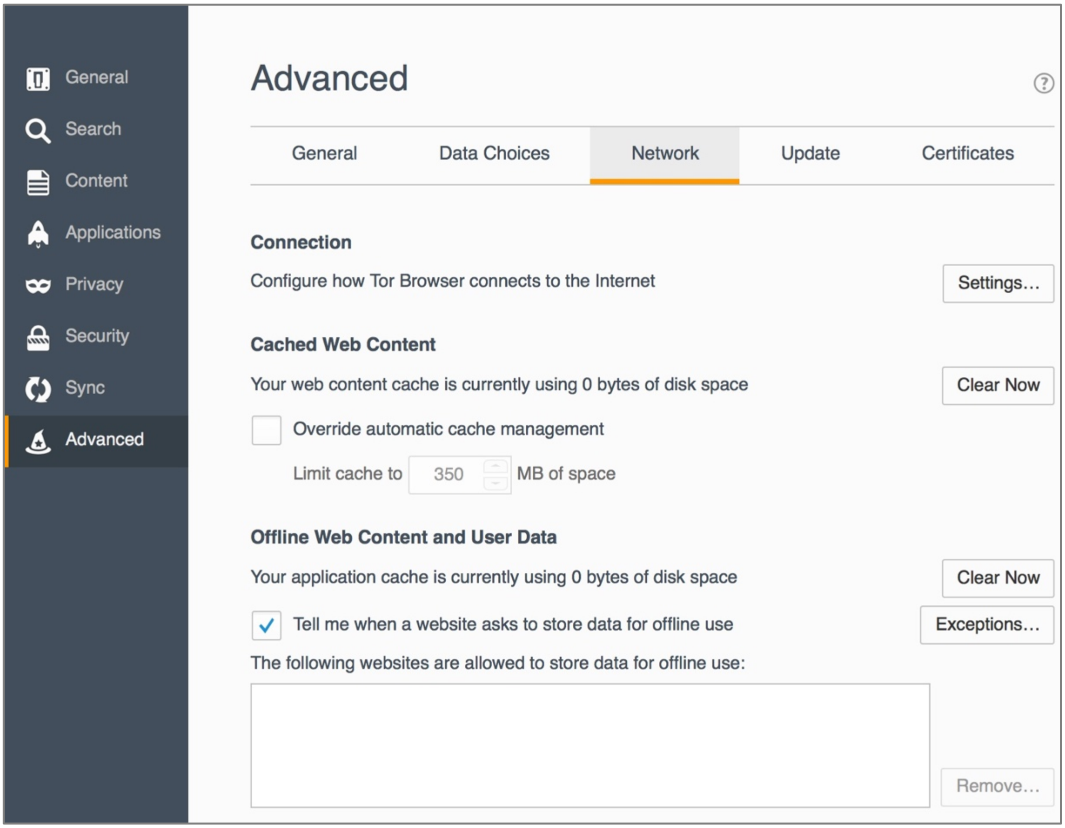
Advanced

☑ **Enable Tor Browser Health Report**

Helps you understand your browser performance and shares data with Tor Project about your browser health

Learn More

10. Select the *Network* tab.



Advanced

Connection

Configure how Tor Browser connects to the Internet

Cached Web Content

Your web content cache is currently using 0 bytes of disk space

□ Override automatic cache management

Limit cache to 350 MB of space

Offline Web Content and User Data

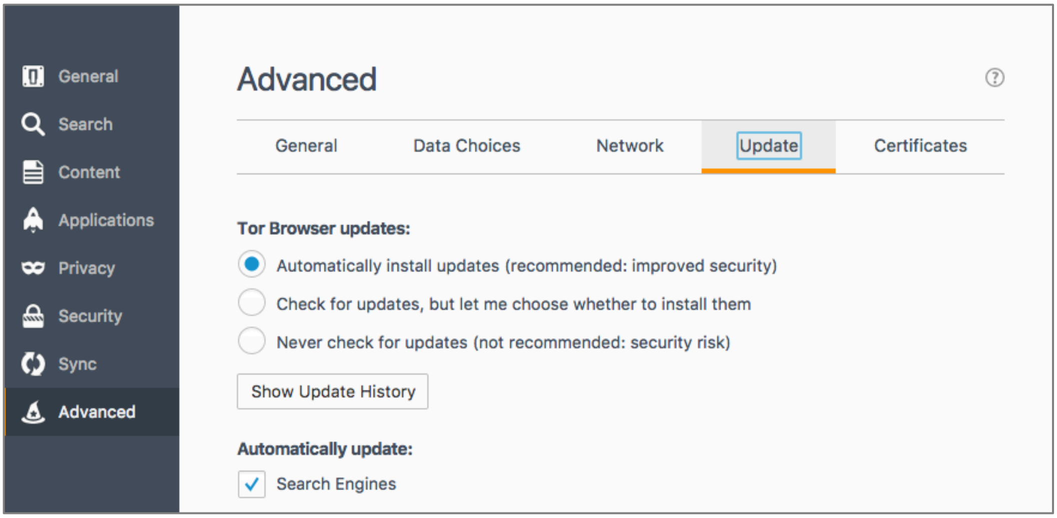
Your application cache is currently using 0 bytes of disk space

☑ Tell me when a website asks to store data for offline use

The following websites are allowed to store data for offline use:

- Enable *Tell me when a website asks to store data for offline use.*
- Configure other settings to your taste.

11. Select the *Update* tab.



Advanced

Tor Browser updates:

● Automatically install updates (recommended: improved security)

○ Check for updates, but let me choose whether to install them

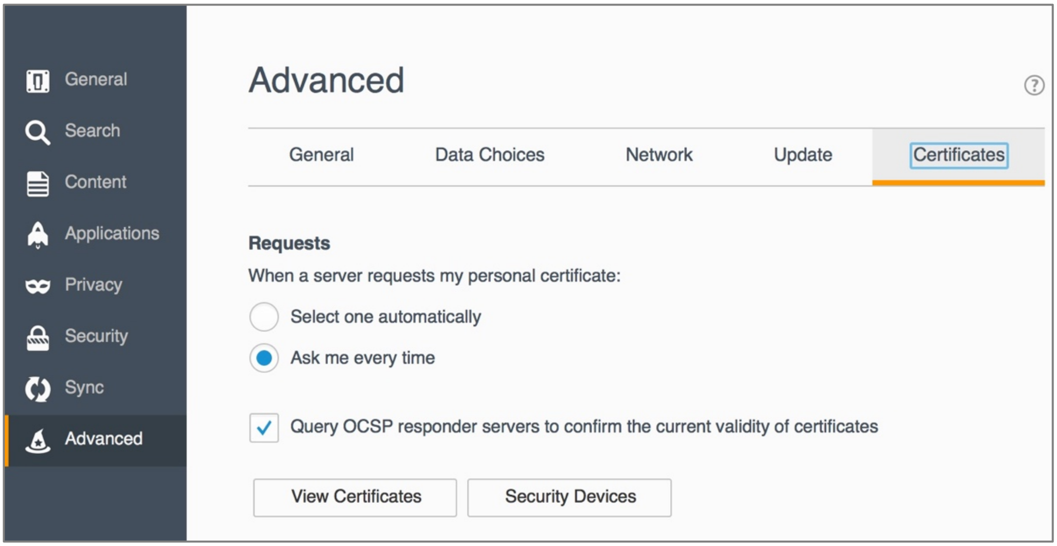
○ Never check for updates (not recommended: security risk)

Automatically update:

☑ Search Engines

- Enable *Automatically install updates (recommended: improved security).*
- Enable *Warn me if this will disable any of my add-ons.*
- Enable *Automatically update: Search Engines.*
- Configure other settings to taste.

12. Select the *Certificates* tab.



Advanced

Requests

When a server requests my personal certificate:

○ Select one automatically

● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

- Enable *Requests > Ask me every time.*
- Enable *Query OCSP responder servers to confirm the current validity of certificates.*

13. Close the preferences tab in Tor.

Great work! You are now ready to use Tor to securely and anonymously browse the Internet.

But remember, Tor is just one small part of *real* anonymity and security on the Internet. Many in the Internet Security field (including Edward Snowden) believe that to do this right, you will want a bootable Tails thumb drive. Learn all about it in our upcoming *Practical Paranoia: Tails Security Essentials* book. In the meantime, visit the Tails[13] home page.

[13] *https://tails.boum.org*

14.12 Onion Sites and the Deep Web

Tor not only allows you to have anonymous access to your regular web sites, it is also the only gateway to the *Deep web*[14]. The deep web is also known as the *Invisible Web*. It consists of web content deliberately not indexed with standard search engines, and only accessible by Tor. These sites are also called *Onion sites*, as they end with *.onion*.

Although the deep web is primarily thought of as a collection of sites to sell illegal products and services, there are also good and responsible uses for it. For example, in repressive countries such sites provide an avenue for freedom workers to work, for reporters to securely exchange information with sources (Ed Snowden did this), and there are sites to provide resources for whistleblowers.

As the deep web is not indexed by Google, Bing, or any other standard search engine, how do you go about discovering its resources? The list is in constant flux, but as of this writing, here are some good starting points:

- TorLinks[15]
- Torch[16]
- Torch Tor Search[17]

[14] *https://en.wikipedia.org/wiki/Deep_web_(search)*
[15] *http://torlinkbgs6aabns.onion*
[16] *http://xmh57jrzrnw6insl.onion/*
[17] *http://torchtorsearch.com*

14.13 Have I Been Pwned

"WHAT!?!" is probably the first thing that just went through your mind. No, it's not a typo. *Pwn*, as defined in the dictionary, is to be totally defeated or dominated. Although most commonly used when trouncing your online game opponent, it is also used to describe when your email or online accounts have been hacked.

And there is a pretty good chance that you have been pwned!

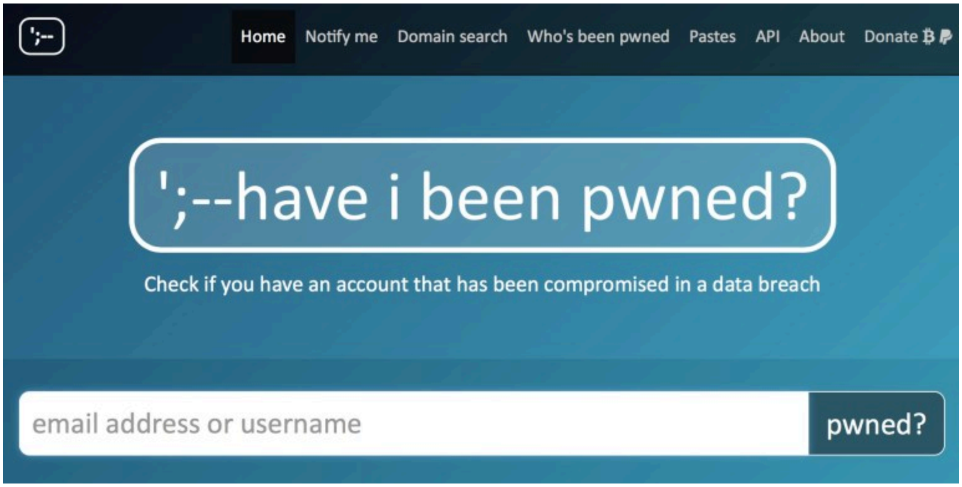
There are several websites that track email and online account breaches. My favorites are *haveibeenpwned* and *hacked-emails.com*.

In this assignment, you search the *haveibeenpwned.com* database to discover if any of your online accounts have been hacked/pwned/breached.

14.13.1 Assignment: Has Your Email Been Hacked

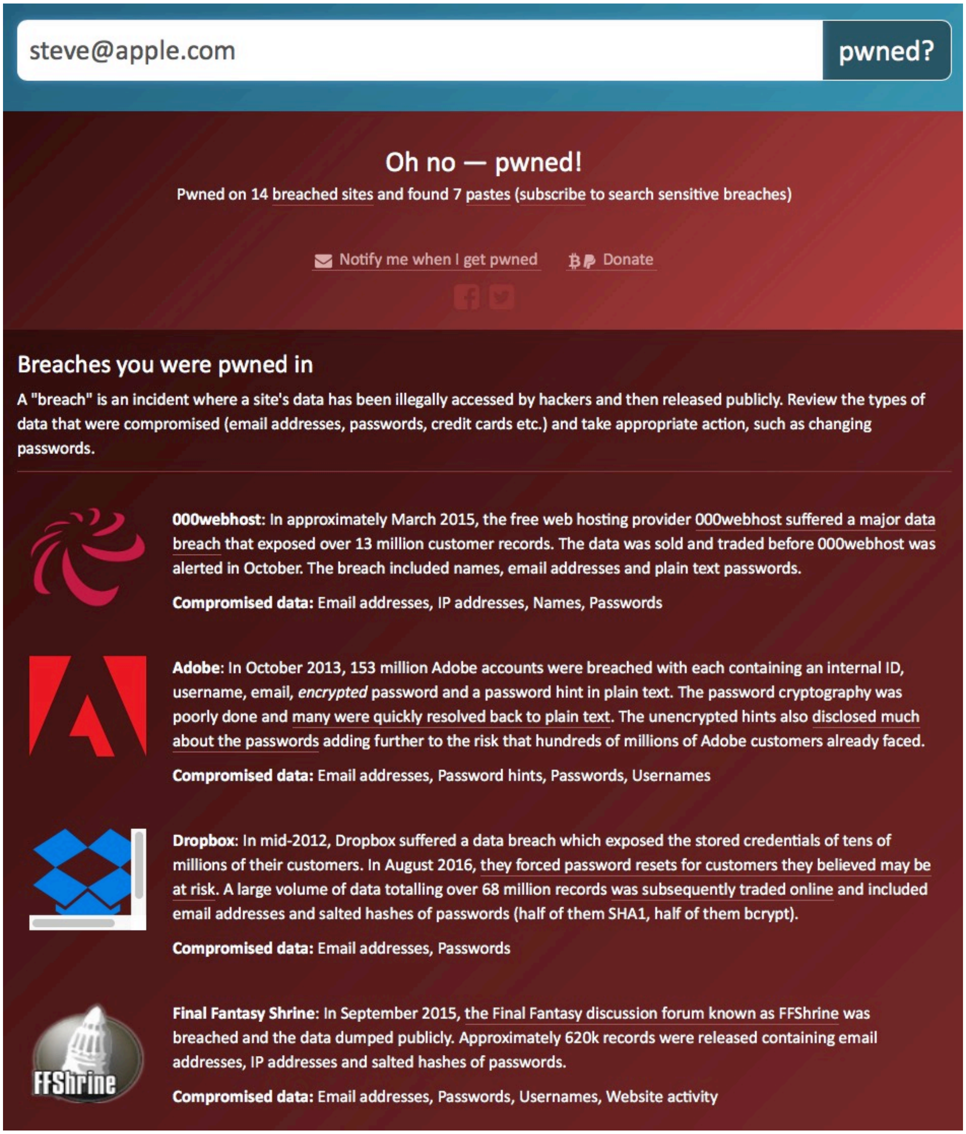
In this assignment, you search the haveibeenpwned.com and hacked-emails.com databases to discover if any of your online accounts have been hacked/pwned.

1. Open a web browser to *https://haveibeenpwned.com*. The home page appears.



2. Enter your email address, and then click the *pwned?* Button.

3. In a few seconds, the results will display.



steve@apple.com

Oh no — pwned!

Pwned on 14 breached sites and found 7 pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed over 13 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Compromised data: Email addresses, IP addresses, Names, Passwords

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

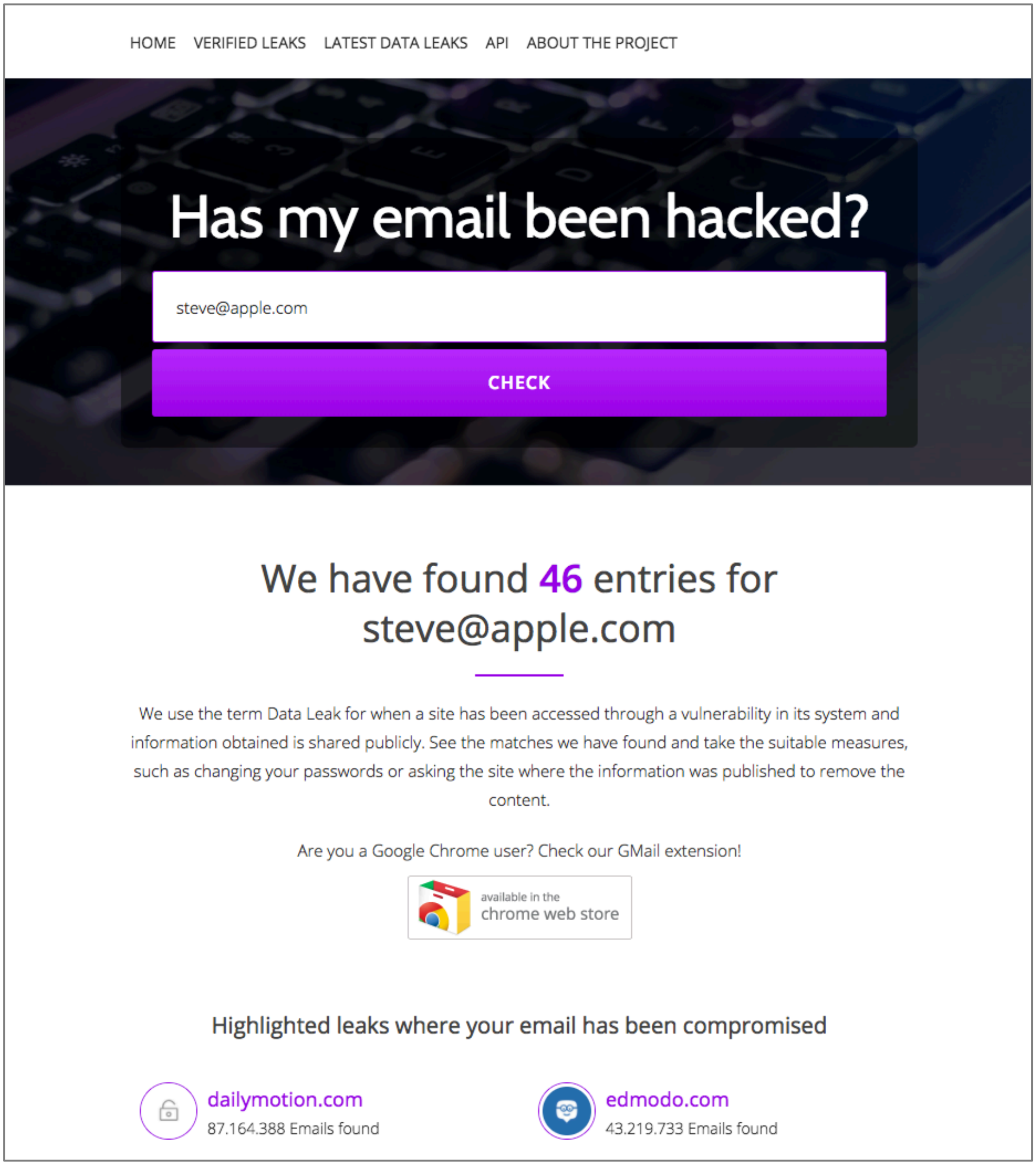
Compromised data: Email addresses, Passwords

Final Fantasy Shrine: In September 2015, the Final Fantasy discussion forum known as FFShrine was breached and the data dumped publicly. Approximately 620k records were released containing email addresses, IP addresses and salted hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames, Website activity

4. Make a note of the sites with breaches.
5. In your browser, go to *https://hacked-emails.com.*
6. Enter your email address, and then click *Check.*

7. All found breaches will display.



Has my email been hacked?

steve@apple.com

We have found 46 entries for steve@apple.com

We use the term Data Leak for when a site has been accessed through a vulnerability in its system and information obtained is shared publicly. See the matches we have found and take the suitable measures, such as changing your passwords or asking the site where the information was published to remove the content.

Are you a Google Chrome user? Check our GMail extension!

Highlighted leaks where your email has been compromised

dailymotion.com
87.164.388 Emails found

edmodo.com
43.219.733 Emails found

8. Close your browser.

14.13.2 Assignment: What To Do Now That You Have Been Breached

In this assignment, you take action to repair any found breaches.

- Prerequisites: Completion of the previous assignment.

1. Open a web browser, and then go to the first breach site.
2. Change your account password, following best practices:
    - Passphrase is a minimum of 15 characters, in an easy to remember, easy to enter phrase.
    - Use the password/passphrase for only one site. Should a site become compromised and your password harvested, the automated hacking systems will use your credentials at every bank, online store, etc. to see if you are like most folks, using one password for everything.
    - Keep a secure record of your passwords/passphrases. I personally like to use *LastPass* as my password manager. Using a current version of *Excel* to create an encrypted spreadsheet also works well.
    - Only enter a username and password when in a secure web page (https).
3. Repeat steps 1 & 2 for each breached site.

15.1 The Killer App

It can be rightfully argued that email is the killer app that brought the Internet out of the geek world of university and military usage and into our homes (that is, if you can ignore the overwhelming impact of Internet pornography.) Most email users live in some foggy surreal world with the belief they have a God or constitutionally given right to privacy in their email communications.

No such right exists. Google, Yahoo!, Microsoft, Comcast, or whoever hosts your email service all are very likely to turn over all records of your email whenever a government agency asks for that data. In most cases, your email is sent and received in clear text so that anyone along the dozens of routers and servers between you and the other person can clearly read your messages. Add to this knowledge the recent revelations about PRISM[2], where the government doesn't have to ask your provider for records, the government simply *has* your records.

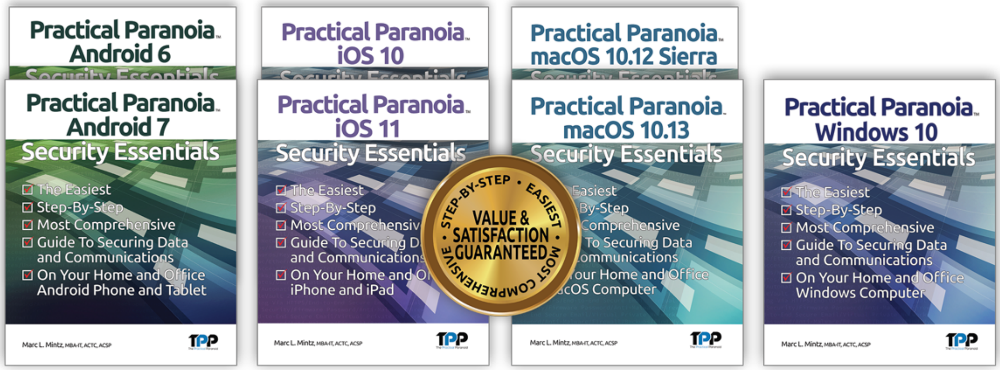
If you find this as distasteful as I do, then let's put an end to it!

[2] *https://en.wikipedia.org/wiki/PRISM_(surveillance_program)*

Index

Practical Paranoia Workshops & Books

4 Years Undisputed #1 Best, Easiest, & Most Comprehensive Cybersecurity Series


Practical Paranoia Android 6 Security Essentials
Practical Paranoia iOS 10 Security Essentials
Practical Paranoia macOS 10.12 Sierra Security Essentials
Practical Paranoia Android 7 Security Essentials
□ The Easiest
□ Step-By-Step
□ Most Comprehensive
□ Guide To Securing Data and Communications
□ On Your Home and Office Android Phone and Tablet
Practical Paranoia iOS 11 Security Essentials
On Your Home and Office iPhone and iPad
Practical Paranoia macOS 10.13 Security Essentials
On Your Home and Office macOS Computer
Practical Paranoia Windows 10 Security Essentials
On Your Home and Office Windows Computer
STEP-BY-STEP • EASIEST • MOST COMPREHENSIVE
VALUE & SATISFACTION GUARANTEED
Marc L. Mintz, MBA-IT, ACTC, ACSP
TPP

This is an age of government intrusion into every aspect of our digital lives, criminals using your own data against you, and teenagers competing to see who can crack your password the fastest. Every organization, every computer user, everyone should be taking steps to protect and secure their digital lives.

The *Practical Paranoia: Security Essentials Workshop* is the perfect environment in which to learn not only *how*, but to actually *do* the work to harden the security of your macOS and Windows computers, and iPhone, iPad, and Android devices.

Workshops are available online and instructor-led at your venue, as well as tailored for on-site company events.

Each Book is designed for classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, and security checklist. Available from Amazon (both print and Kindle format), and all fine booksellers, with inscribed copies available from the author.

Call for more information, to schedule your workshop, or order your books!

The Practical Paranoid, LLC
+1 888.504.5591 • info@thepracticalparanoid.com
https://thepracticalparanoid.com