

Browsing the Web More Securely & More Privately With Firefox On Your Mac

DRAFT Version 0.1
April 28th, 2014

Joe St Sauver, Ph.D.
(joe@uoregon.edu)

<http://pages.uoregon.edu/joe/browsing-securely-mac-firefox/>

Disclaimer:

This document represents the opinions of its authors, and not necessarily the opinion of any other entity.

It is provided on a best-effort basis, as-is, where-is, with all faults, errors and omissions.

Given the complexity of individual systems and the diverse and constantly changing nature of the Internet threat landscape, even if you perfectly follow all the recommendations in this document we CANNOT guarantee that you'll be able to use the Internet completely securely and completely privately.¹

Therefore, if you decide to use the Internet, whether you follow the recommendations in this document or not, you do so SOLELY AT YOUR OWN RISK.

¹ According to <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/> 59% of Internet users do not believe it is possible to be completely anonymous online.

Table of Contents

I.	INTRODUCTION	6
I-1.	Why is web security important?	7
I-2.	Why is this document needed?	8
I-3.	What's the "right" level of security and privacy for a typical user?	9
I-4.	Choices about your security may impact your privacy	11
I-5.	Security and privacy impacts: mitigate via product design?	12
I-6.	Choices about security may impact <i>more</i> than "just" privacy	13
I-7.	Another example of tradeoffs: the Tor Browser Bundle	14
II.	THREAT MODEL	16
II-1.	Security and privacy threat <u>sources</u>	17
II-2.	In-scope threats	18
II-3.	Out-of-scope threats	20
II-4.	Maintaining your security and privacy requires taking an "ecosystem-wide" perspective	21
III.	OPERATING SYSTEM RECOMMENDATIONS	23
III-1.	Malware is one factor driving your choice of operating system	23
III-2.	Picking a non-MS Windows operating system option	24
III-3.	Browsing with a guest operating system within a virtual machine	25
IV.	HARDENING MAC OS X	27
IV-1.	Backups	27
IV-2.	Basic Patching	28
IV-3.	Patching Other Software	30
IV-4.	Antivirus Software	31
IV-5.	Whole Disk Encryption	32
IV-6.	Using a firewall to block unwanted traffic	33
IV-7.	Cleanup your cached files, log files, etc.	35
IV-8.	Cover your camera	36
IV-9.	Mute your microphone	37
IV-10.	Install a privacy filter over your display	38
IV-11.	What About Using a "Locate My Lost or Stolen Laptop" Program?	38
IV-12.	Install A Firmware Password?	38
V.	SECURING ACCOUNT-RELATED ITEMS	39
V-1.	Create a non-admin account for routine use; don't browse from an admin account	39
V-2.	Make sure your system's passwords are long, strong, and unique	40
V-3.	Ensure that the "root" user in Mac OS X isn't enabled	41
V-4.	Don't "cache" sudo status by default	41
V-5.	Guest account	42
V-6.	Use a password manager/password safe	42

VI.	SECURING LOGIN-WINDOW-RELATED ITEMS	43
VI-1.	Configure the system login preferences for security	43
VI-2.	Warning banners	44
VI-3.	Activate Active Screen Corners for locking your screen	45
VI-4.	Review and Disable Any Unneeded Login-Time/Boot-Time Automatically-Launched Items ...	46
VII.	CONFIGURING NETWORK CONNECTIVITY	47
VII-1.	Disable all unneeded network interfaces	47
VII-2.	Review and adjust network connectivity settings as appropriate	47
VII-3.	Connect directly, not via a local/enterprise proxy server	49
VII-4.	Use a 3rd Party VPN?	51
VII-5.	Use Tor?	51
VIII.	OTHER SYSTEM PREFERENCES AND MISCELLANEOUS TWEAKS	52
VIII-1.	Confirm that sharing is disabled	52
VIII-2.	Ensure O/S privacy settings are appropriate	52
VIII-3.	Ensure that Date & Time are NOT set to "set time and time zone automatically."	52
VIII-4.	Eliminate "Recent" Items	53
VIII-5.	Print Jobs: Disable List of Print Jobs	53
VIII-6.	Clear shell history in terminal	53
VIII-7.	Confirm that user home directories aren't group or world readable or traversable	54
VIII-8.	Disable the Spotlight local search engine	54
VIII-9.	Securely delete any files in the trash	55
IX.	LEARNING MORE ABOUT SECURING MAC OS X	56
IX-1.	Additional Mac operating system security/privacy reading	56
IX-2.	Subscribe to the Apple security announcement mailing list	56
X.	SECURING THE WEB BROWSER (FINALLY!)	57
X-1.	Picking the "most secure" browser	57
X-2.	What's LEFT as a possible browser option?	59
X-3.	Review browser privacy policies	61
X-4.	Check to make sure Firefox is the default browser on startup	62
X-5.	Keep Firefox patched up-to-date	63
X-6.	Plugins/browser extensions	64
X-7.	Recommended plugins/browser extensions	65
X-8.	Ad-Block Plus	66
X-9.	Ghostery	66
X-10.	NoScript	67
X-11.	Better Privacy	68
X-12.	Certificate Patrol	69
X-13.	RefControl	70
X-14.	Changing the user agent string	71
X-15.	Patching plugins, browser extensions and helper apps	73
X-16.	Configuring the browser for better <u>security</u>	75
X-17.	Warn me when sites try to install add-ons	75
X-18.	Block reported attack sites; block web forgery sites	75
X-19.	Do NOT use "remember passwords for sites"	76

X-20.	Block pop-up windows	76
X-21.	Choose helper applications for file types	77
X-22.	Personal certificate privacy	77
X-23.	Recommended browser preference settings for improved <u>privacy</u>	78
X-24.	Set a blank home page or use a privacy-preserving search engine as your start page	78
X-25.	Tell sites that I do not want to be tracked, always use private browsing mode & reject cookies	79
X-26.	Disable local cached web content	80
X-27.	Connect directly, not via a proxy server	81
X-28.	Do not enable telemetry, health reports or crash reports	82
X-29.	Device synchronization features	82
X-30.	Secure Web Sites and SSL/TLS Support in Firefox	83
X-31.	Firefox Support for TLS 1.2 and Strong Ciphers with Forward Secrecy	83
X-32.	Ensure that OCSP/CRL is used (and required, if possible)	84
X-33.	Trust anchors	84
X-34.	Firefox making connections w/o me doing anything????	85
X-35.	Protecting the User's Privacy: browser fingerprinting	85

XI. DEEP SETTINGS: FIREFOX AND ABOUT:CONFIG SETTINGS 86

I. INTRODUCTION

*Nothing ever comes for free
This world is watching me
* * **

*Now all that's left is all I need,
This world is watching me*

Armin van Buuren, "This World Is Watching Me"

You'd like to be able to use your computer to ***safely and securely***, particularly for browsing the web. For example:

- You'd like to be able to freely surf the Internet without worrying that you'll get infected with malware.
- It should be possible for you to safely use your computer to make online purchases, or to safely do online banking or to manage your stock portfolio.
- Hacker/crackers shouldn't be able to remotely scan your system and find exploitable vulnerabilities.
- If your system gets stolen, a thief shouldn't be able to access the information contained on it.

You'd also like to be able to use your computer ***privately***, without being monitored and tracked. This includes:

- Being able to search the web and visit web sites without worrying that your every move is being tracked and recorded.
- Being able to use your computer without have it eavesdrop on your activities via its camera, microphone or geolocation capabilities.
- Hardening your network connectivity against eavesdropping.
- Protecting your system against those who may want to rummage through files stored on your system, if given the opportunity to potentially do so.

This document is meant to help moderately technical users who are security- and privacy-focused make progress toward achieving the above security and privacy goals when using an Apple Mac with the Mozilla Firefox browser.

A version of this document may be prepared for selected other operating system/browser combinations at a later date.

In the mean time, particularly if you're on a PC running Microsoft Windows and you're privacy/security concerned, you may want to investigate use of Tails (a bootable live operating system) as an alternative.²

² <https://tails.boum.org/>

I-1. Why is web security important?

Laptop users tend to spend more time in their web browser than any other Internet application.³

Users routinely use their browsers to connect to potentially risky sites of unknown provenance -- and then use the same browser (now potentially tainted) to connect to highly security-sensitive sites.

As such, the web browser has become one of the most heavily targeted vectors for attacks on user security and privacy.^{4, 5}

We know, for example, that the American intelligence community (IC) is confident that they can use the web browser to compromise "targets of interest," if they can just get them to visit a "booby-trapped" web site. This attitude can be seen in the remark:⁶

“If we can get the target to visit us in some sort of web browser, we can probably own them,” an agency hacker boasts in one secret document. “The only limitation is the ‘how.’”

When this document was initially undertaken, we'd (naively) hoped to be able to recommend just a few minor configuration changes. We'd hoped that those changes would be enough to substantially improve user security and privacy when using the web, while still leaving users with a browser usable for most popular web sites.

Over time, while writing this document, we came to understand that that was a naive and unrealistic goal.

³ Not sure this is true in your case? Try a time tracking application such as <http://manytricks.com/timesink/>

⁴ "Browser-based threats dropped to 45 percent of all attacks we measured, compared with 73 percent last quarter...", <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf> at PDF page 20.

⁵ <http://www.zdnet.com/security-2014-the-holes-are-in-the-apps-not-the-operating-systems-7000026893/> mentions "A Secunia study revealed that Web-browsers, and other Internet-connected programs, as you'd expect, are the source of most attacks. Web browsers, as always, are under near constant attack. There's a reason why Google and HP are offering more than \$3-million in awards for hackers who can break the most popular browsers at Pwn2Home and Pwnium security conferences."

⁶ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

I-2. Why is this document needed?

Describing how to actually secure a typical user's web browser is a surprisingly complicated process, and many popular web sites (including most Alexa Top 100 U.S. web sites⁷) require users to run with features that are inherently unsafe/privacy-hostile. This includes, but isn't limited to, sites that require users to:

- Register or login to access resources such as trial software or whitepapers,⁸
- Accept tracking cookies,⁹ or
- Allow JavaScript¹⁰ and Flash.¹¹

This is partially a reflection of the fact that these technologies meet legitimate needs (e.g., it is hard to deploy interactive web-based applications without JavaScript), but it is also a reflection of the fact that many parts of the Internet rely on advertising for revenue.

The requirements of online marketers -- *and* the requirements of the intelligence community (IC), law enforcement (LE) agencies, and hacker/crackers -- have some disturbing parallels, including the fact that all of those entities would like to be able to track/monitor your online activities.

The upshot of this commonality of interest is that many of the needs of the IC, LE agencies, and hacker/cracker communities have already been "baked into" the products you use, and the software you may install and routinely run.

If you want to enjoy a modicum of online security and privacy, you may need to work hard to "back out" those insecure defaults, and you may need to make some hard choices about what you're willing to forgo in order to get the security and privacy you may want or need.

⁷ <http://www.alexa.com/topsites/countries/US>

⁸ Most commonly, this is done to:

- (a) Make it possible for an online application to save state (e.g., user preferences) across visits to a site,
- (b) Provide a mechanism for things like password recovery if a site-specific password is forgotten,
- (c) Record consent to various policies (e.g., site copyright/software non-redisclosure agreements),
- (d) Discourage anonymous spamming (e.g., in blog comment areas), or to
- (e) Allow sales representatives to obtain "leads" to individuals who might be interested in purchasing a product or service.

Nonetheless, the potential privacy impact of requiring registration (and the enhanced "trackability" it enables) is impossible to overlook.

⁹ "June 2012 Web Privacy Census," <http://www.law.berkeley.edu/14496.htm>

¹⁰ <http://w3techs.com/technologies/details/cp-javascript/all/all> says that JavaScript is used by 87.7% of all sites.

¹¹ <http://w3techs.com/technologies/details/cp-flash/all/all> says that Flash is used by 14.3% of all sites

I-3. What's the "right" level of security and privacy for a typical user?

How much privacy and/or security should a user intentionally forgo in order to be able to continue to use useful web resources? While there will be many subtle intermediate gradations, the four basic options are:

-- ***Users Can Simply Ignore Online Security Issues:*** This is what all too-many people do by default. Perhaps due to being overwhelmed, many people just **ignore** online security and privacy issues entirely. They've given up, and will allow the ebb and flow of the security tides to carry them wherever they may happen to go, including potentially out into deep, cold, and dangerously stormy waters. This is a passive approach.

-- ***Users Can Take "Reasonable" (If Less Than Perfect) Precautions:*** This will probably be the most common option for those who are interested in/concerned about security and privacy. Users of this sort will run with a browser configuration that is as secure as possible -- while still being compatible with the sites they want or need to be able to use. In making these choices, they will explicitly or implicitly accept that they may be vulnerable to some attacks. We might call this the "mainstream" security choice. In choppy waters, they're wearing their life preservers.

-- ***Users Can Adopt a Strict "Security-Oriented Lifestyle:"*** This means that users will configure their system and browser for maximum security and privacy, recognizing that doing so means they'll need to forgo core functionality on at least some web sites. For example, with JavaScript disabled, much of Google won't work (or won't work very well). Continuing our maritime metaphor, these users might have a survival suit on board, or stay in the harbor if a severe storm is expected off shore.

-- ***You Can Disconnect From the Internet Entirely:*** While this is an extreme choice, it is one that some entities do actually make. (Once again, this means that folks have effectively given up -- but in a different way than those who simply pretend security isn't an issue.) For example, critical infrastructure providers, sensitive government defense and intelligence systems, etc., are routinely partitioned from the public Internet. Most average users, however, won't find this to be an appropriate/proportionate response to the security and privacy threats that they face. In our maritime metaphor, these users will have put their boats in dry dock, and no longer go out to sea at all, and that's a shame. A boat that's out of the water is safe, but that's not why we buy boats.

We can graphically represent that continuum as shown in Figure 1:

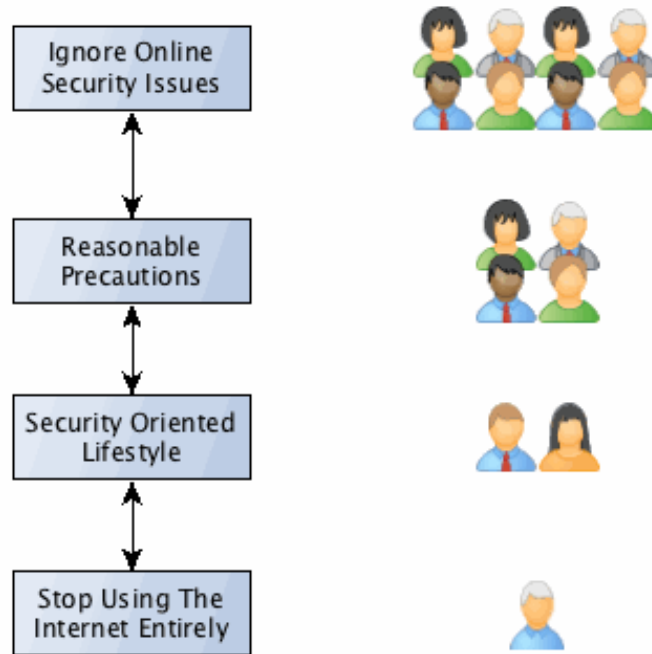


Figure 1: When It Comes To Security And Privacy on the Internet, What Do Most People Choose?

As shown in the figure above, most users will do nothing. Some will take reasonable precautions. A smaller number still will adopt a security oriented lifestyle. A few (hopefully *just* a few) may even decide to disconnect from the Internet entirely.

While we'd probably prefer to see most users adopt a "security oriented lifestyle," we'd even be happy if more people simply took "reasonable precautions."

We **don't** want you to see you **either** totally ignore security and privacy issues **nor** do we want to see you stop using the Internet entirely -- there are simultaneously too many threats **and** too much that's good and worthwhile to either just pretend the Internet is totally safe, or to pretend that the right choice is just to disengage from the Internet entirely.

Ultimately, however, only you can decide what's right for your work, your computer, and you.

This document is meant to help you with those choices, and to help you improve your security and privacy online.

I-4. Choices about your security may impact your privacy.

In making choices about your *security*, those choices have the potential to negatively impact your *privacy*.

Example #1: For example, imagine a hypothetical "ad supported" web site reputation browser toolbar from a trusted vendor. That toolbar offers to review the domain names of web sites you're about to visit, blocking any that it recognizes as malicious.

By blocking malicious sites, the hypothetical toolbar would help you avoid sites known to be infected with malware, and known phishing sites.

Thus, installation of that toolbar would potentially help improve the *security* of your browser.

Of course, if the toolbar wasn't from a trustworthy vendor, your security could actually be made worse (e.g., if the toolbar was actually malicious software), or if the toolbar had its own security-related bugs).

On the other hand, by running that toolbar, your *privacy* will almost certainly be made *worse*: a third party (e.g., the browser toolbar service operator) will now be able to see the domain names of the sites you visit, including those that may be potentially privacy-sensitive in nature.

And naturally, it would probably not be surprising if targeted ads seen from that advertising-supported toolbar were correlated with the sort of sites you visit: that is, if you tend to visit a lot of web sites about flying, you might expect to see ads for planes, flight schools, avionics, magazines about flying, gadgets for pilots, etc.

Thus, you can see that improved *security* from the browser toolbar may come at a cost to your *privacy*.

If the browser toolbar vendor is reputable, and the vendor doesn't abuse the stream of data they receive from you, you may decide to accept that "cost."

Alternatively, you may simply decide not to use that toolbar, perhaps picking an alternative toolbar with a different/more privacy-preserving design.

I-5. Security and privacy impacts: mitigate via product design?

Instead of a hypothetical toolbar that sends each URL back to the toolbar vendor for evaluation, imagine an alternative toolbar with a *different* architecture.

Example #2: In the case of this alternative product, rather than sending each URL back to the toolbar vendor in real time, the toolbar periodically pulls down and locally installs a copy of a "bad domain" file, much as antivirus products download antivirus definitions.

Having done that, the alternative toolbar then wouldn't have to send any sensitive information about what you're browsing back to the operator of the toolbar, the toolbar could just check the domain names against that local file.

But that architecture has tradeoffs as well:

- If you only download a new list of bad sites once a day, that list won't protect you against the most recent bad domains, and if an important good site is accidentally listed, it may take nearly a day for that error to get corrected. That can be a long time for a good site to wait to be "pardoned."

- That list may also be large and time consuming to download, listing tens of thousands or even hundreds of thousands of domains that you may never visit or need to evaluate, and taking up more storage space than you might like (at least on space constrained mobile devices)

Obviously there's no perfect solution, and no "free lunch."

I-6. Choices about security may impact more than "just" privacy.

While the tension between security and privacy is the one that's most often mentioned, there are other competing objectives that may also be impacted. For example, coming back to our original hypothetical browser toolbar that's doing "real time" checks for bad domain names, using that toolbar may impact...

-- *Performance may be made worse.* Since you won't go to the web site you're trying to visit until the remote toolbar site review server receives the domain name from your browser, analyzes it, and returns a signal that the site is safe, web performance may take a hit (whether or not this impact is material may vary from user to user, perhaps depending on their location and connectivity). In addition to worsening normal transactional latency, the user's ability to browse may be blocked entirely if the toolbar's reputation server can't be reached for an opinion, or the toolbar's reputation server farm becomes overloaded and slow to respond, etc.

-- *Usability may be made worse.* To understand why, note that the hypothetical browser toolbar does its assessment on a domain-name-wide basis. That means that it may block access to ALL pages on a domain name if there's even ONE phishing or malicious page on that domain name.

-- *Simplicity may be made worse.* If the hypothetical browser toolbar is potentially incompatible with the new version, at browser upgrade time it will be temporarily unusable/disabled until it can be made compatible with the new version of the browser.

As another example, imagine a partisan group that decides to intentionally flag their opposition's web sites as malicious, even if they are in fact entirely innocuous. A user thus needs to consider the possibility that a badly-rated/blocked site is actually not dangerous, but merely ideologically disliked by a subset of raters.

-- *Cost may potentially go up.* While there's no "up front"/"out of pocket" cost to using this advertising sponsored toolbar, you are exposed to advertising that helps to underwrite its costs. That *is* a "cost," albeit one paid in your time/attention, lost screen real estate, and irritation, rather than cash. (There's also the possibility that you may actually in fact buy something you see advertised).

We can symbolize these tensions as shown in Figure 2:

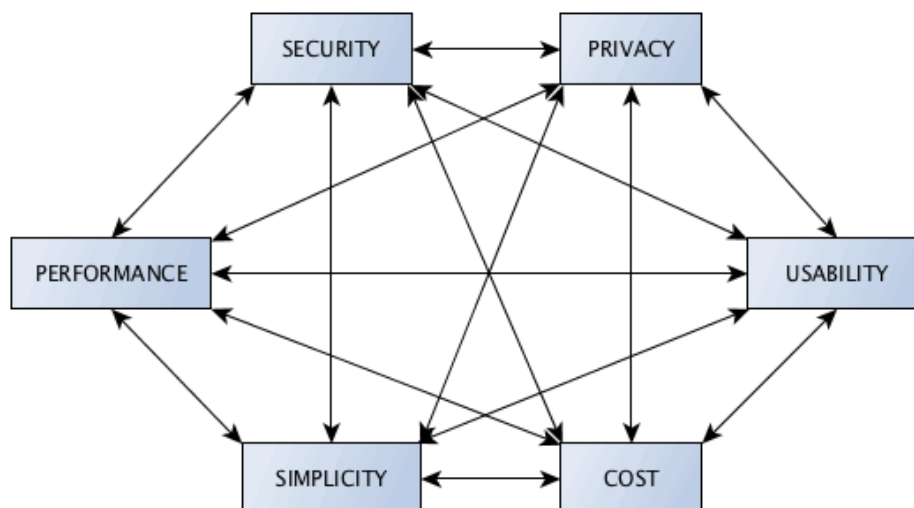


Figure 2: The Tension Between Security, Privacy, Performance, Usability, Simplicity and Cost

I-7. Another example of tradeoffs: the Tor Browser Bundle.

Example #3: Suppose that you're a privacy-oriented person, and you were thinking about using the Tor Browser Bundle¹² in an effort to defeat traffic analysis-related threats against your online privacy. How might that impact each of the six areas that are in tension?

-- *Privacy: mixed.* Your privacy will be improved when it comes to defeating traditional traffic analysis, since Tor-ified traffic passes through multiple hops between entering the encrypted Tor network and exiting onto the regular Internet. However, at the same time, there's also the possibility that an untrustworthy entity operating a Tor exit node may sniff (or attempt to sniff) your traffic and thereby potentially compromise your privacy¹³ in a way that might not have occurred if you hadn't used Tor. We also know that use of Tor repeatedly increases the chance that your encrypted traffic will be captured and retained by the NSA, even if it might otherwise not be.¹⁴ The result is thus a bit of a mixed bag, privacy-wise.

-- *Security: also mixed.* Let us begin by saying that the Tor project makes an aggressive attempt to deliver a high level of practical security and privacy for its users, as discussed in the Tor Browser Design Guide.¹⁵ We applaud that effort.

We also know that the NSA is reportedly rather frustrated with Tor, as revealed by documents that Edward Snowden reportedly provided to The Guardian.¹⁶

At the same time, there has also been at least one successful attack on the security of the Tor Browser Bundle.¹⁷

Reportedly, too, if you use Sophos on your Mac you may also need to disable protection from "malicious websites" and "malicious downloads" in order to be able to use Tor.¹⁸

-- *Performance: worse.* Browsing with Tor tends to be consistently slower than when browsing without Tor.¹⁹

¹² <https://www.torproject.org/projects/torbrowser.html.en>

¹³ <https://www.torproject.org/docs/faq.html.en#CanExitNodesEavesdrop> and

<http://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/>

¹⁴ <http://arstechnica.com/tech-policy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-data/>

¹⁵ <https://www.torproject.org/projects/torbrowser/design/>

¹⁶ "NSA and GCHQ target Tor network that protects anonymity of web users," <http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>

"Tor Stinks' presentation -- read the full document," <http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>

¹⁷ <https://lists.torproject.org/pipermail/tor-announce/2013-August/000089.html>

¹⁸ <https://www.torproject.org/docs/faq.html.en#SophosOnMac>

¹⁹ <https://www.torproject.org/docs/faq.html.en#WhySlow>

-- *Usability: worse.* For example, the Tor Project's FAQ includes an item, "Why can't I view videos on YouTube and other Flash-based sites?"²⁰

See also the discussion of why Tor does not recommend using other Firefox extensions (including ad blocking software),²¹ and note the way that Google sometimes requires that you solve a CAPTCHA when using Tor through some exit nodes.²²

IPv6 support in Tor is also something that's missing but which would be nice to have.²³

-- *Simplicity: worse.* Tor is trying to do something that's inherently complex, and is balancing a variety of competing requirements. Just to mention one example, Tor blocks some ports by default.²⁴

As another example, Google sometimes selects the wrong language/version by default when your exit node is in some other country.²⁵

-- *Cost: mixed.* Tor is free software, but clearly you will "pay" a price that involves a variety of non-monetary costs.

Some users may also prefer to buy a hardware implementation of Tor, such as the \$49 PogoPlug SafePlug.²⁶ Obviously in that case, there are easily quantifiable out-of-pocket costs.

To conclude this section, we hope you'll note that in all of these examples, improving security and privacy requires accepting other tradeoffs.

As you decide on how much security and/or privacy you want or need, ***strive to understand all the implications of the choices you make.***

In many cases you may face "tricky choices" where there is no "universally right" answer.

²⁰ <https://www.torproject.org/docs/faq.html.en#TBFlash>

²¹ <https://www.torproject.org/docs/faq.html.en#TBOtherExtensions>

²² <https://www.torproject.org/docs/faq.html.en#GoogleCAPTCHA>

²³ <https://www.torproject.org/docs/faq.html.en#IPv6>

²⁴ <https://www.torproject.org/docs/faq.html.en#DefaultExitPorts>

²⁵ <https://www.torproject.org/docs/faq.html.en#ForeignLanguages>

²⁶ <https://pogoplug.com/safeplug>

II. THREAT MODELS

'There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know.'

Donald Rumsfeld, US Secretary of Defense, from a press conference in February 2002

-- -- --

*"[...] if I knew back then what I know right now
There'd be no ifs and buts and no maybes"*

[from the "Saudades de Rock" album by the rock band Extreme]

We now want to talk a little about the threat models that are relevant and which help to frame and shape the contents of this paper.

In discussing these threats we need to recognize that we don't (and can't!) definitively know all relevant threats. We need to do our best to understand the potential threats given what information is available, and proceed on that basis.

II-1. Security and privacy threat sources.

Many of the security and privacy threats you face online come from mundane sources, including:

- Online marketers/advertisers
- Technical staff members (webmasters, network engineers, information security officers, etc.)
- Colleagues/co-workers, and friends/family members
- Academic network researchers.

Other security and privacy threats you may face online may come from more chilling sources:

- Hackers/crackers, botmasters, and other cyber criminals
- Law enforcement (and/or regulatory) agencies, or
- Foreign (or domestic!) intelligence services.

At a practical level, all of those security and privacy threat sources use similar approaches to compromise your security and privacy, and require similar approaches to mitigate or thwart.

As a result, work to manage security and privacy threats experienced by law abiding adults may inadvertently and unavoidably interfere with things like:

- carefully-conducted responsible academic research,
- good faith efforts by parents to protect innocent children from disturbing or even dangerous online content, or
- court-authorized law enforcement efforts targeting violent criminals.

We're sorry about that sort of potential "collateral damage," but those unintended consequences aren't enough to make us abandon our efforts to explain how law-abiding adults can at least attempt to improve their security and privacy online.

II-2. In-scope threats.

While we'd like to be able to address all possible web-related threats, we can't. Therefore, we need to decide what security and privacy threats are "in-scope" and which are "out-of-scope."

- a. One in-scope threat category consists of *technical vulnerabilities* associated with the user's operating system, web browser, web browser plugins, etc. These technical vulnerabilities may be exploitable either by malware, or in some cases by direct scan-and-spoit attacks conducted over the network.
- b. A second in-scope threat category consists of *pervasive monitoring*. This includes:

-- *Web analytics* (web server log analysis, use of "cookies"²⁷ (including so-called "supercookies" or "evercookies"²⁸), web bugs²⁹ (unique transparent tracking pixels planted in and automatically loaded when web pages are viewed), user agent data³⁰ and browser fingerprinting techniques,³¹ mining of referrer data,³² use of geolocation data,³³ and particularly use of Google Analytics³⁴)

-- *Traffic analysis* (analysis of source and destination IP addresses and port numbers, session start and stop times, octets transferred, etc., but NOT THE CONTENTS of the traffic).

Traffic analytic approaches often leverage data routinely captured via NetFlow.³⁵

Law enforcement officers often refer to this sort of an approach as a "pen register/trap and trace (PR/TT),"³⁶ and the intelligence community may refer to this as "metadata-based approaches."³⁷

-- *Network eavesdropping* (monitoring of the full contents of network traffic, e.g., perhaps by forcing all web traffic through a corporate web proxy or web gateway, or through use of an Ethernet span port or passive optical tap to obtain a copy of network traffic). Criminal law enforcement officers conducting this sort of monitoring normally call this a "Title III" "full contents" intercept.³⁸

²⁷ http://en.wikipedia.org/wiki/HTTP_cookie

²⁸ <http://en.wikipedia.org/wiki/Evercookie>

²⁹ http://en.wikipedia.org/wiki/Web_bug

³⁰ http://en.wikipedia.org/wiki/User_agent#Possible_privacy_issue

³¹ <https://panopticklick.eff.org/>

³² http://en.wikipedia.org/wiki/HTTP_referer#Referer_hiding

³³ <http://www.mozilla.org/en-US/firefox/geolocation/>

³⁴ <http://www.google.com/analytics/>

³⁵ <http://en.wikipedia.org/wiki/NetFlow>

³⁶ <http://www.law.cornell.edu/uscode/text/18/part-II/chapter-206>

³⁷ <http://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama>

³⁸ http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00028.htm

c. A third threat category that's in-scope consists of *local or in-person attacks*, such as:

-- *Unauthorized or surreptitious access to systems*, including review and/or duplication of information on systems during international border crossings³⁹ (but NOT the surreptitious installation of physical "bugs" or surveillance hardware -- that's out of scope for this document).

-- *Device forensics*,⁴⁰ perhaps done with Encase⁴¹ or a similar forensic analysis tool, intended to "carve out" (recover):

- files cached by the web browser,
- lists of recently visited web sites,
- web cookies indicative of a user's browsing habits,
- passwords stored accessibly in some web browsers,⁴² and
- incompletely deleted/non-overwritten files.⁴³

-- *Local wireless monitoring*, including use of tools such as Aircrack-NG⁴⁴ or Firesheep⁴⁵

-- *Shoulder surfing* (e.g., watching what's shown on someone else's screen or what they type)

-- *Unauthorized access to information stored on lost or stolen devices*.

d. A fourth threat category consists of *social engineering attacks*, most commonly "phishing" (e.g., a user may be presented with a web site that looks like his or her bank, but which is actually controlled by an attacker seeking to compromise the person's banking credentials).

e. The fifth and final threat category consists of *web filtering/network censorship*. This may be nation-state filtering,⁴⁶ or policy-based local filtering, such as may be done for some K12 audiences by schools⁴⁷ or by some parents to protect their minor children.⁴⁸

³⁹ <https://www EFF.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices>

⁴⁰ One example of the most popular tools used for this purpose is EnCase; a list of other forensic tools can be seen at http://en.wikipedia.org/wiki/List_of_digital_forensics_tools

⁴¹ <http://www.guidancesoftware.com/>

⁴² <http://www.engadget.com/2013/08/07/chrome-saved-passwords/>

⁴³ For example, see Disk Drill from <http://www.cleverfiles.com/>

⁴⁴ <http://en.wikipedia.org/wiki/Aircrack-ng>

⁴⁵ <http://codebutler.com/firesheep/>

⁴⁶ <http://freedomhouse.org/report/freedom-net/freedom-net-2013>

⁴⁷ For example, see http://en.wikipedia.org/wiki/Children%27s_Internet_Protection_Act

⁴⁸ http://en.wikipedia.org/wiki/Parental_controls

II-3. Out-of-scope threats.

While the preceding section makes clear that there are many privacy and security areas that are "in-scope" for this document, there are other areas that are explicitly "out-of-scope," including:

a. *Privacy-infringing revelations that you or others may voluntarily make via social media* (e.g., on Facebook, LinkedIn, Google+, etc.). We can't protect you from the consequences of what you (or your friends and family) choose to voluntarily disclose. If you are privacy and security aware, our general recommendation would be to avoid using social media, and to ask your friends and family to omit references to you, photos of you, etc., from what they say. You should note that some people may consider a *lack* of social media presence to be unusual, and if they notice it, that anomaly may cause them to "dig deeper" about you through alternative channels.

b. *Other personal choices you knowingly and intentionally make that negatively impact your security.* For example, if you decide to share the administrative password to your laptop with a family member who ultimately proves to be untrustworthy, that misplaced trust is not something we can prevent.

c. *Server-side issues.* If there are technical issues on the "other side" of your network connection, you're not going to be able to fix those. We may help you *identify* that those problems exist, but ultimately *fixing* those issues is something that's on someone else's shoulders. This includes:

- Web server software (Apache, Microsoft IIS, etc.) vulnerabilities⁴⁹
- Web application errors (e.g., web apps with OWASP Top 10 programming flaws⁵⁰)
- Web performance/scaling issues (including dealing with distributed denial of service attacks),⁵¹ and outright web site outages due to power problems, fiber cuts, etc.
- Regulatory/compliance requirements pertaining to web sites (e.g., FTC Children Online Privacy Protection Act (COPPA) requirements,⁵² etc.)

d. *Hardware security-hindering/privacy-violating vulnerabilities*, including things like the installation of hardware key logging devices,⁵³ and (at the extreme) *electromagnetic emissions security vulnerabilities* on non-TEMPEST hardened/typical consumer-grade systems.⁵⁴ While we're talking about hardware-related vulnerabilities, we explicitly note that we will assume that you do not have the ability to irreversibly modify/intentionally break the hardware you're using. Thus, for example, we will NOT be including some "staple" recommendations often encountered in high security environments, such as physically disconnecting any integrated camera and microphone, or plugging USB ports with silicone sealant to prevent insertion of thumb drives, etc.

e. *Judicially-compelled disclosures* are out of scope, as is *so-called "Rubber hose cryptography."*⁵⁵

⁴⁹ For example: http://httpd.apache.org/security/vulnerabilities_24.html

⁵⁰ https://www.owasp.org/index.php/Top_10_2013-Top_10

⁵¹ For example: <http://en.wikipedia.org/wiki/Slowloris>

⁵² <http://www.business.ftc.gov/privacy-and-security/childrens-privacy>

⁵³ See for example <http://www.keelog.com/> , <http://www.keyghost.com/> , <http://www.keycatcher.com/> , etc.

⁵⁴ http://en.wikipedia.org/wiki/Tempest_%28codename%29

⁵⁵ <http://xkcd.com/538/>

II-4. Maintaining your security and privacy requires taking an "ecosystem-wide" perspective.

If you attempt to just secure your laptop, your web browser, and your network connection, that may not be enough to protect your security and privacy.

To understand what we mean by this, let's consider some brief scenarios:

a. Your web browser is only secure as the least secure add-on you've added to it

If you have a web browser that would be secure in-and-of itself, but you install an insecure add-on, you will now have a web browser that's no longer secure. This is also true if you misconfigure your web browser, or fail to periodically clean up cached files and log files it creates, etc.

b. Like many people you carry and use a smart phone as well as a laptop.

If your laptop is tightly buttoned down and highly secure, but your smart phone is *not*, your smart phone may have insecurities that undercut your overall security and privacy posture. For example, even if you've made it difficult or impossible for your laptop to be used to track your physical location (or to be used as a surreptitious eavesdropping device), that won't matter if your smart phone (which you also routinely carry) allows you to be geolocated and/or eavesdropped upon.

c. You connect through an insecure home wireless "router"/gateway.

If that "choke point" isn't secure, all the traffic through that choke point may be intercepted or modified.

d. Family members (or colleagues) with their own systems share the network connection you use.

Even if *your* laptop is secure, if your family members (or colleagues) also have laptops that *aren't* (and those systems share your same network connection), their laptops may end up being used to invade your privacy, or may end up being used as a stepping stone from which to launch a successful attack against the security or privacy of your system (or your network traffic)

e. You use an insecure email account.

If you voluntarily use a \web email account that's been identified as part of the NSA PRISM program,⁵⁶ for example, your expectations for the privacy of that account should be low or non-existent -- and that vulnerability may be a "gap in your defenses" that can then be used to undercut all (or much) of the rest of your security and privacy. Important note: at least some of the providers identified as having been compelled to participate in PRISM have now taken affirmative steps to protect their user community.

f. You use a credit card to make online purchases.

If you use a traditional credit card issued in your real name to make online purchases, those purchases will go far toward tying all related online activities to your real identity.⁵⁷

g. You don't shred your snail mail, printed output, disks, thumb drives, etc., before throwing them away.

⁵⁶ http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

⁵⁷ Assume that the act of making an online purchase ties together (a) the IP address you're using, (b) your real world identity as shown on the credit card, (c) your email address as well (used for confirming your order, etc.), (d) your shipping address, plus (e) information about your purchasing habits.

Some may make the mistake of only thinking about electronic/online security, and ignore physical security. "Dumpster diving"⁵⁸ and "trash covers"⁵⁹ never seem to go out of style, unfortunately, and a surreptitiously installed video camera located near where you routinely use your computer can be extremely privacy invasive.

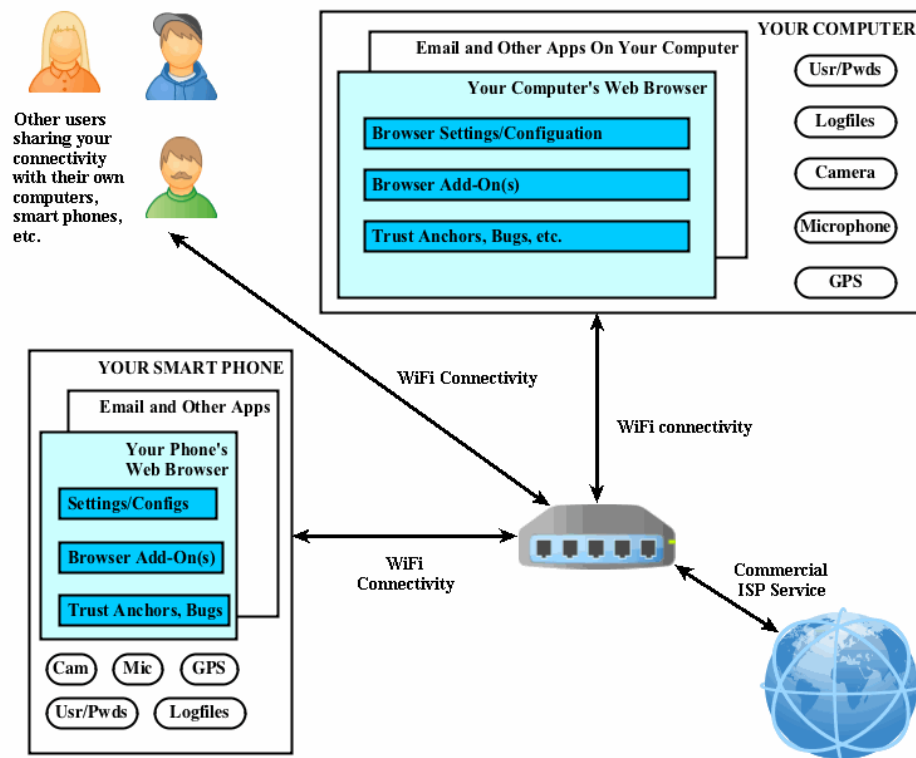
h. *You fail to ask to have your personal data removed from various online "white page" or "online directory" resources; see the opt-out pointers at <https://www.abine.com/optouts.php>*

If you want to use the Internet in a secure and private way, ultimately you need to look at ALL the elements of your lifestyle and local environment, and ensure that *everything* you do is security- and privacy-favorable.

Note that in some cases you may already have enough Internet "history" that it may be hard for you to retroactively establish a high level of security and privacy without essentially going through the Internet equivalent of the Federal Witness Protection Program.⁶⁰

See the simplified diagram below.

The (Simplified) Local Threat Ecosystem



⁵⁸ http://en.wikipedia.org/wiki/Garbage_picking

⁵⁹ http://en.wikipedia.org/wiki/Garbology#Investigative_uses

⁶⁰ http://en.wikipedia.org/wiki/United_States_Federal_Witness_Protection_Program -- critically important witnesses in high profile criminal cases may be relocated and given new identities by the authorities to protect them from witness intimidation or attacks by the criminals against whom they'll be testifying. The Internet equivalent would entail getting all new hardware, new connectivity, new accounts, new credit cards for online use, etc.

III. OPERATING SYSTEM RECOMMENDATIONS

Before we can talk about securing your browser, you need to have a secure operating system to act as a sound foundation upon which it can run.

Browsers run on top of an operating system, most commonly some version of Microsoft Windows or Mac OS X, but also possibly Linux (or another flavor of Unix, such as NetBSD, FreeBSD, or OpenBSD).

The security of the system as a whole depends on the security of the operating system (and your network connection) *as well as* the security of the browser.

So what operating system should you use?

III-1. Malware is one factor driving your choice of operating system

While there are many different ways that a system can become compromised, **malware** has consistently been one of the most important threats to system security and privacy. Most malware is dropped on users by cyber criminals, but malware has also been leveraged by intelligence agencies to eavesdrop on selected targets. As Glenn Greenwald has written:⁶¹

[W]hat the Der Spiegel article details is that one of the things that the NSA is really adept at doing is implanting in various machines—computers, laptops, even cellphones and the like—malware. And malware is essentially a program that allows the NSA, in the terminology that hackers use, to own the machine. So, no matter how much encryption you use, no matter how much you safeguard your communication with passwords and other things, this malware allows the NSA to literally watch every keystroke that you make, to get screen captures of what it is that you're doing, to circumvent all forms of encryption and other barriers to your communications.

Therefore, avoiding malware (whether dropped by criminals or some other entity) is absolutely key to creating an environment where security or privacy is possible. If you do get infected with malware, any steps you may try to take to "secure" your system will ultimately be pointless unless/until you've mitigated your malware infection.

When most users think about combatting malware, their first thought is to use a commercial antivirus product.

Technical security people know that most commercial signature-based antivirus products are only partially effective at best, and in some cases, detection rates may be disappointingly low.⁶²

Therefore, it's critically important for you to run an operating system that is incompatible with most of the malware that's currently in circulation. If you run something *other than* Microsoft Windows your risk of getting infected with malware decreases dramatically since virtually ALL laptop/desktop malware targets only Microsoft Windows.⁶³

⁶¹ Glenn Greenwald: The NSA Can "Literally Watch Every Keystroke You Type," December 31, 2013, <http://truth-out.org/news/item/20948-glenn-greenwald-the-nsa-can-literally-watch-every-keystroke-you-make>

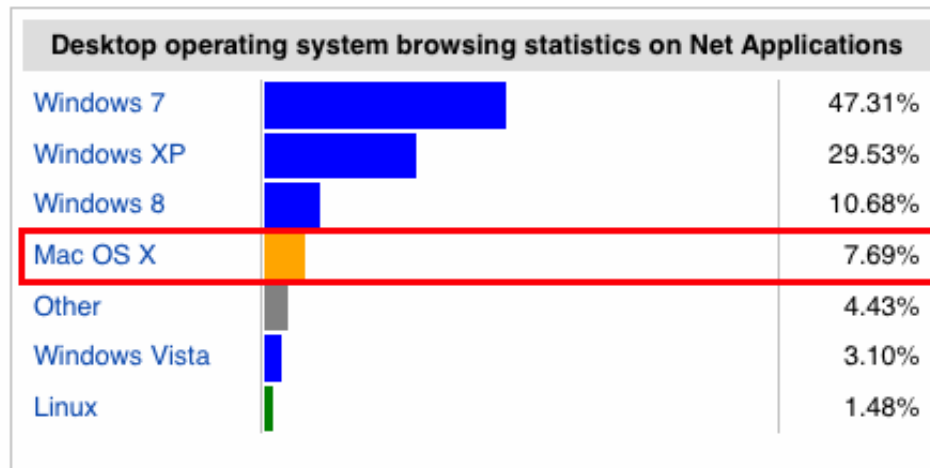
⁶² "Antivirus software is not enough to prevent a cyber attack: during a month long cyber attack by Chinese hackers on the New York Times, the company's antivirus software missed 44 out of the 45 pieces of malware installed by attackers on the network," <http://money.cnn.com/2013/01/31/technology/security/antivirus/>

⁶³ Nice historical overview of Mac malware at <http://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/>

III-2. Picking a non-MS Windows operating system option.

Although the prevalence of malware-related threats may be enough to render MS Windows an unacceptably risky choice, how are we to figure out which of the remaining operating systems we should use, instead? For example, should security conscious users be running Mac OS X, some version of Linux, some version of BSD (OpenBSD, FreeBSD, NetBSD, etc.), or perhaps even something else, such as ChromeOS?

As a practical matter, if you eliminate all versions of MS Windows, the only operating system with at least a 5% market share is Mac OS X:⁶⁴



We also note that that the above market share report is a broad one. If you look just at U.S. higher education, it isn't uncommon to see Macs running 1-to-1 in adoption relative to MS Windows.⁶⁵

While we recognize that Linux, BSD and ChromeOS all have unique advantages that make them potentially attractive for security-conscious users, we believe that they're too atypical to routinely recommend for privacy-conscious users. (You don't want to be atypical enough that a webmaster can identify you simply by scanning his web logs for the one visitor who routinely connects from a host that's running an unusual operating system, right?)

Mac OS X also has the advantage of supporting the sort of native productivity applications (such as Microsoft Office) that many business or higher users may find to be "must haves."

For the remainder of this whitepaper, as a security and privacy-oriented person, we assume that you'll be using a Mac running OS X, and if you ever attend a cybersecurity-related event, you'll see that's what most of the attendees at those events in fact use.

⁶⁴ http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

⁶⁵ By way of example, the University of Wisconsin states at <https://kb.wisc.edu/showroom/page.php?id=3045> that "Roughly 50% of college students last year on our campus had Mac computers."

III-3. Browsing with a guest operating system within a virtual machine.

If you run in a virtual machine (VM) and something bad happens, that badness may be limited to just that VM. In that case, you can just delete your current snapshot to clean up your "mess."

<https://www.virtualbox.org/> (a GPL free/open source software product) is one example of a virtual machine that a moderately technical user could use for this purpose. (Note: in recommending that you consider using a virtual machine, I am assuming that you will be running a free/open source guest operating system such as some version of Linux)

VIRTUAL MACHINE

Security	+
Privacy	+
Simplicity	--
Cost	-
Usability	-
Performance	--

Targeted risk: infection of base operating system.

a. Download and install VirtualBox.

Download the Mac OS X version of VirtualBox from <https://www.virtualbox.org/wiki/Downloads>

Once the download completes, double click on the dmg file in Firefox --> Tools --> Downloads

Double click on the VirtualBox.pkg file in the installation window that opens, installing the program for all users.

b. Select, download and install the guest operating system you'd like to run.

You can see examples of pre-built open source images that you could run within VirtualBox at <http://virtualboxes.org/images/> [note that this name is similar to, but different than the preceding site]

You'll need to have UnArchiver⁶⁶ installed to decompress the 7z-compressed pre-built open source image files.

For example, maybe you'd like to run FreeBSD 7.1. It is available via a link from <http://virtualboxes.org/images/freebsd/> When you download it and UnArchiver uncompresses that file, you'll be left with a disk image named "FreeBSD-7.1-i386.vdi"

Now launch VirtualBox by double clicking on /Applications/VirtualBox.app

Click the "New" blue seal in the VirtualBox Manager.

Enter "FreeBSD" in the "Name" field.

Set Type to BSD, and Version to FreeBSD (64 bit). Click Continue.

On the Memory size screen, leave the memory set to 128MB. Click Continue.

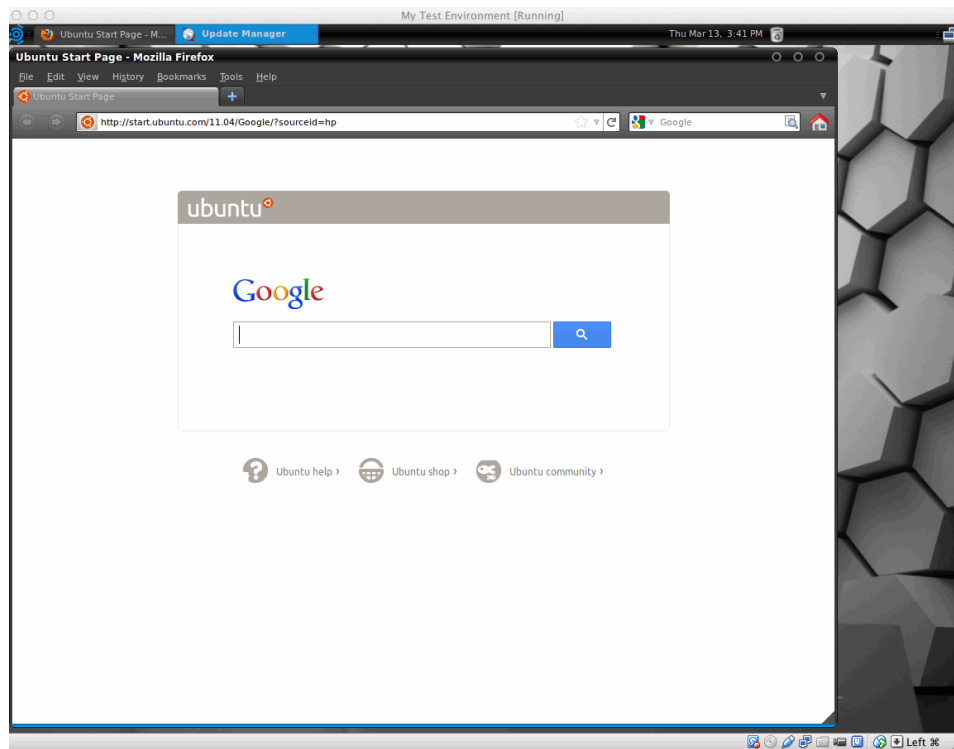
On the Hard drive screen, select "Use an existing virtual hard drive" and then click on the file folder icon to navigate to the file "FreeBSD-7.1-i386.vdi"

Click "Create."

Double click on "FreeBSD" in the left hand column of the Virtual Box Manager to launch the image. Be patient while FreeBSD loads.

The default username/password for that image, as noted on the web site, are root/toor, User/devil

⁶⁶ <http://wakaba.c3.cx/s/apps/unarchiver>



When considering use of a virtual machine environment, note that you will want to make sure that you have sufficient CPU horsepower and sufficient physical memory for adequate performance, and enough disk space to accommodate a second operating system and duplicate applications, etc.

Be sure you also recognize that you'll *ALSO* need to patch and secure the guest operating system just as you patch and secure the underlying host operating system -- don't try this approach unless you're willing to be conscientious about that extra work.

IV. HARDENING MAC OS X

IV-1. Backups.

Backups are critically important. Periodically backup your system so that if your system is lost or stolen, or it becomes malware infected, or a patch goes badly, or an antivirus product malfunctions, etc., you can easily restore your system from a recent backup.

Before you do anything else, PLEASE BACK UP YOUR SYSTEM!

And, after you've got everything configured the way you want it, take ANOTHER backup as a checkpoint to save all your hard work, and then schedule at least weekly backups thereafter (and don't overwrite your old backups! KEEP your old backups!)

Backups should be encrypted to ensure that loss of a backup doesn't result in a breach.

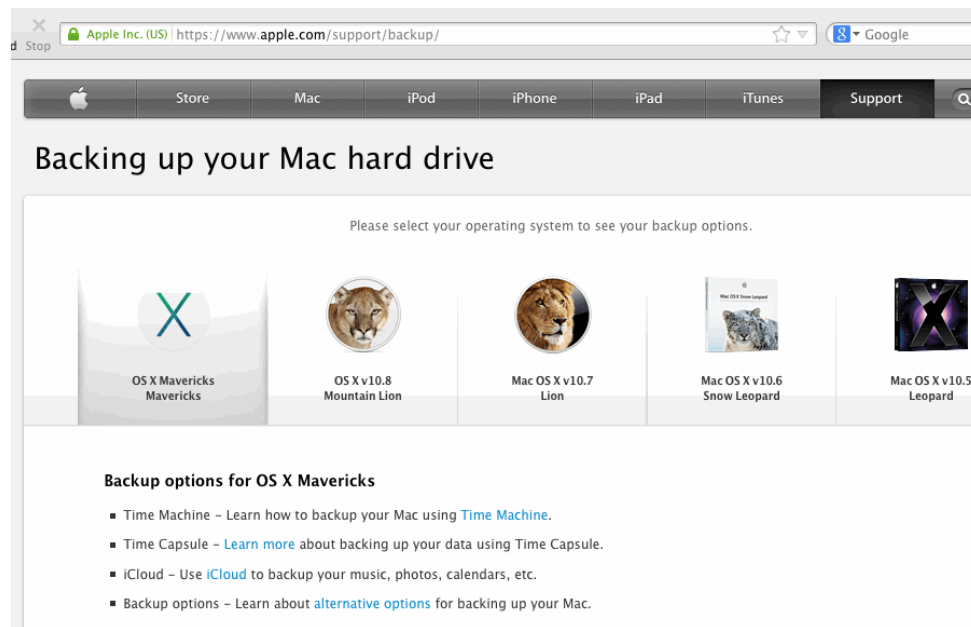
Backups are particularly important these days due to "CryptoLocker"⁶⁷ and similar ransomware -- if you don't have clean recent backups, malware that encrypts critical files on your system can really hurt you.

For information on backing up your Mac, see <https://www.apple.com/support/backup/>

BACKUPS

Security	+++
Privacy	-
Simplicity	-
Cost	-
Usability	0
Performance	0

Targeted risk: irrecoverable data loss



⁶⁷ <http://en.wikipedia.org/wiki/CryptoLocker>

IV-2. Basic patching.

Patches are critical when it comes to protecting you from known vulnerabilities. While we can talk about lots of other far more subtle things, basic patching is absolutely key.

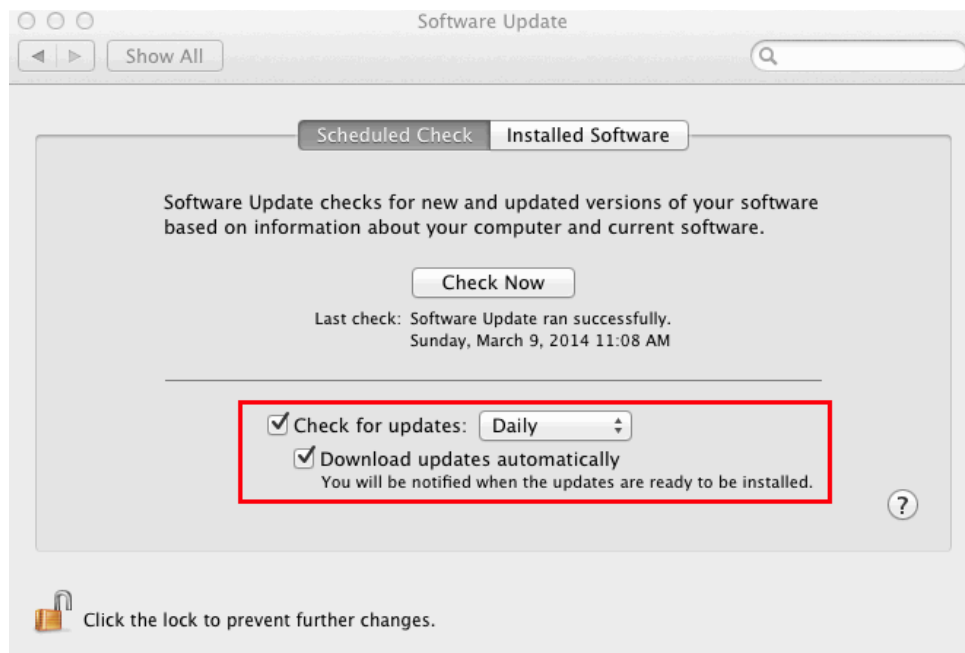
-- *Major OS Version:* Run the most recent version of OS X available from Apple. At this time, that would be OS X Mavericks, available for free from <https://www.apple.com/osx/> (Note that only relatively current systems will be able to run OS X Mavericks.) Many people still haven't upgraded.⁶⁸

-- *Ensure You've Applied Apple Automatic Software Updates:* Go to System Preferences --> Software Update --> Scheduled Check. Make sure that "Check for Updates" is selected. Set the frequency to "Daily." Also check to make sure that "Download updates automatically" is also checked. Finally, click "Check Now" to make sure that you're current right now. Apply any available updates.

PATCHING

Security	+++
Privacy	-
Simplicity	-
Cost	-
Usability	0
Performance	0

Targeted risk: bugs resulting in unauthorized access



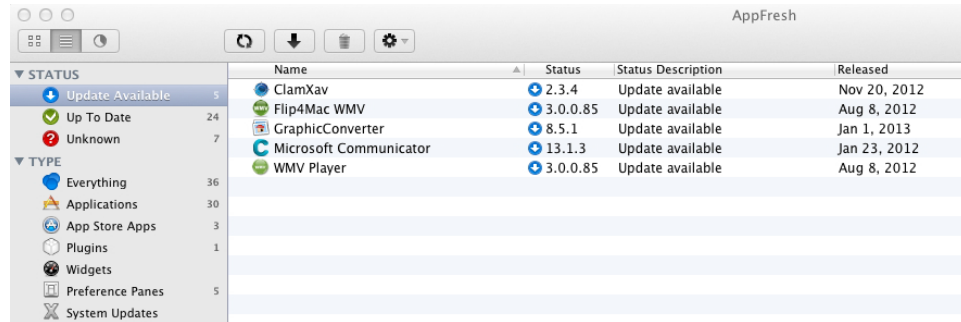
-- *App Store Updates:* Many users may have applications downloaded from the Apple App Store. To check for updates for those applications, go to the Apple menu in the upper left hand corner, run "App Store..." and click on "Updates" in the App Store.

-- *Microsoft Office:* Microsoft Office will normally automatically check for updates when it is run, however you can manually check for updates by running an Office application (such as Microsoft Word), and then going to Help --> Check for Updates.

⁶⁸ <http://nakedsecurity.sophos.com/2014/01/09/82-of-enterprise-mac-users-not-getting-security-updates/>

-- *AppFresh for Mac*: AppFresh is a commercial product that can automatically check for updates to most installed products on your Mac. AppFresh is available for a free two week trial, or purchase it for \$14.95 from <http://metaquark.de/appfresh/mac>

An example of what AppFresh might find:



The screenshot shows the AppFresh application window. On the left, there is a sidebar with two sections: 'STATUS' and 'TYPE'. The 'STATUS' section has three items: 'Update Available' (5), 'Up To Date' (24), and 'Unknown' (7). The 'TYPE' section has six items: 'Everything' (36), 'Applications' (30), 'App Store Apps' (3), 'Plugins' (1), 'Widgets' (5), and 'Preference Panes' (5). The main area of the window displays a table of applications with available updates.

Name	Status	Status Description	Released
ClamXav	2.3.4	Update available	Nov 20, 2012
Flip4Mac WMV	3.0.0.85	Update available	Aug 8, 2012
GraphicConverter	8.5.1	Update available	Jan 1, 2013
Microsoft Communicator	13.1.3	Update available	Jan 23, 2012
WMV Player	3.0.0.85	Update available	Aug 8, 2012

Figure 3. Example of Apps Found by AppFresh To Have Available Updates

IV-3. Patching other software.

-- *Apple Developer Tools*: If you've installed the Mac OS/X Developer Tools, go to your /Applications folder and run Xcode , applying any updates that may have been made available (e.g., this may include updates for the command line tools or other applicable components).

-- *X11 Windows Support*: In addition to the Mac's native windowing system, some users also run X11 Windows (the classic Unix windowing system). If so, you can obtain the latest version from <http://xquartz.macosforge.org/trac/wiki/WikiStart>

If you use XQuartz, you may want to get in the habit of periodically checking for/installing the latest version.

-- *Mac Package Managers*: Some users also may have installed software using a so-called "package manager," such as MacPorts. If you're using MacPorts, be sure to periodically open a Terminal window and do:

```
$ sudo port selfupdate
$ sudo port upgrade outdated
```

IV-4. Antivirus software.

While it is true that there's limited Mac malware in circulation, and antivirus products aren't perfect and will routinely miss some infectious files, they may also catch some, so you should routinely use an antivirus product as part of a comprehensive and redundant strategy for dealing with malware, even on a Mac.

Examples of Mac antivirus products free for *home use* (some may be free for any/all systems, check the terms of use carefully) include (in alphabetical order):

-- avast! Free Antivirus for Mac⁶⁹

-- AVG⁷⁰

-- Avira⁷¹

-- ClamXav⁷²

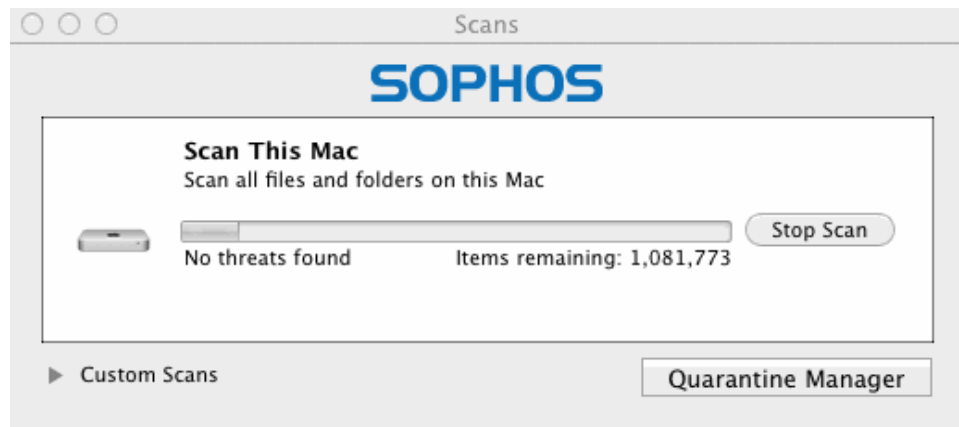
-- Comodo Antivirus for Mac⁷³

-- Sophos Antivirus for Mac⁷⁴

ANTIVIRUS

Security	++
Privacy	0
Simplicity	-
Cost	-
Usability	0
Performance	-

Targeted risk: malware infection.



⁶⁹ <http://www.avast.com/en-us/free-antivirus-mac>

⁷⁰ <http://www.avg.com/us-en/for-mac>

⁷¹ <http://www.avira.com/en/download-start-new/product/avira-free-mac-security>

⁷² <http://www.clamxav.com/>

⁷³ <http://www.comodo.com/home/internet-security/antivirus-for-mac.php>

⁷⁴ <http://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx>

IV-5. Whole disk encryption.

Careful as you may be, systems still end up getting lost or stolen. When that happens, the information stored on those systems will be at risk if those system aren't protected with whole disk encryption. Whole disk encryption also ensures that unauthorized modifications normally can't get surreptitiously made.

Like all security measures, whole disk encryption isn't without "costs." For example, once you've enabled whole disk encryption, you normally won't be able to remotely reboot your system without someone physically available to enter the whole disk password as part of the boot process.

On the Mac, the easiest way to deploy whole disk encryption is by using FileVault, which is built into OS X. (System Preferences --> Security & Privacy --> FileVault Tab --> Turn On File Vault).

Be sure to set a recovery key, and store the recovery key someplace safe.

WHOLE DISK ENCRYPTION

Security	++
Privacy	++
Simplicity	-
Cost	-
Usability	-
Performance	0

Targeted risk: data breach.



Another alternative that more technical users may want to consider is TrueCrypt.⁷⁵

⁷⁵ <http://www.truecrypt.org/>

See also: <http://istruecryptauditedyet.com/>

IV-6. Using a firewall to block unwanted traffic

Firewalls aren't a magic bullet and can't eliminate all threats,⁷⁶ but they at least can be useful when it comes to mitigating classic "scan and 'sploit"-type remote attacks, particularly if the goal is just to reduce the level of attack-related noise that shows up in system log files.

The Mac includes an integrated software firewall, and that's a reasonable first step if you'd like to get at least basic firewall protection deployed.

To enable the Mac's software firewall go to System Preferences --> Security & Privacy --> Firewall Tab --> On.

SYSTEM FIREWALL

Security	++
Privacy	+
Simplicity	--
Cost	0
Usability	-
Performance	-

Targeted risk: system cracked by remote attacker



For fine-grained control, technically inclined users may also consider installing IceFloor.⁷⁷

Little Snitch, a commercial firewall product for the Mac, is another popular option that's also appropriate for technically inclined users.⁷⁸ Unlike other products, Little Snitch pays particular attention to OUTBOUND traffic, which may be important if you're worried about data exfiltration, or are particularly concerned about your privacy as much as your security.

⁷⁶ For a more detailed discussion of firewalls and their limitations, see "Cyberinfrastructure Architectures, Security and Advanced Applications," <http://pages.uoregon.edu/joe/architectures/architecture.pdf>

⁷⁷ <http://www.hanynet.com/icefloor-2.0.zip>

⁷⁸ <http://www.obdev.at/products/littlesnitch/>

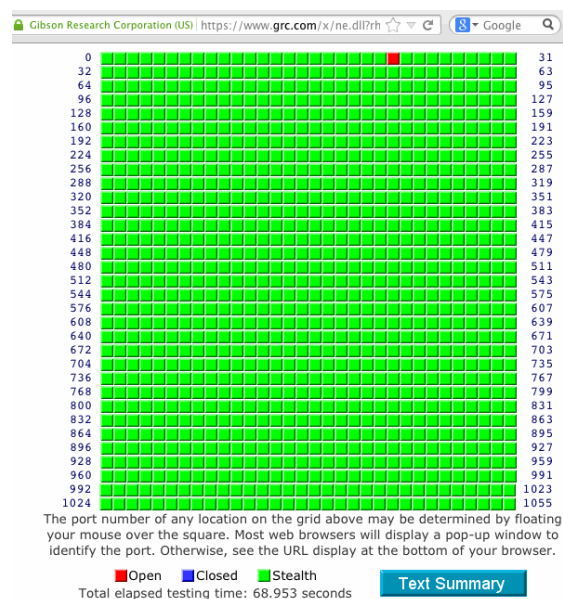
Consider complimenting the software firewall you use with a hardware firewall, even if that's only a basic home "router"/gateway device.⁷⁹

Note that use of a home "router"/gateway device may limit throughput in some cases, and may also hinder your ability to deploy IPv6 unless you're careful to select a device that supports IPv6, such as an Apple AirPort Express.

After enabling and configure your firewall(s), confirm that your firewall(s) is/are working by visiting a remote port scanning site such as GRC's Shields Up.⁸⁰

A typical workstation, when checked with GRC Shields Up, should show **all** ports green/inaccessible.

A GRC Shields Up display for a server that has only one service, sshd, accessible would look like (note the one red square in the matrix):



If you scan your system and see unexpected ports reported as open, take the time to figure out what you're seeing, and work to disable those open ports if you don't intend and require that they be exposed.

⁷⁹ Note that many popular home "router"/gateway devices bundle WiFi wireless service. Whenever possible, you should disable WiFi and connect directly to the gateway device via traditional wired Ethernet.

⁸⁰ <https://www.grc.com/x/ne.dll?bh0bkyd2> (after reading the disclaimer, click Proceed, then "All Service Ports")

IV-7. Cleanup your cached files, log files, etc.

A basic step that's sometimes forgotten is to clean up old cached files, old log files, etc. There's now a Mac version of the popular cleaning tool CCleaner. Use it to periodically clean up the cruft that may otherwise accumulate on your Mac.

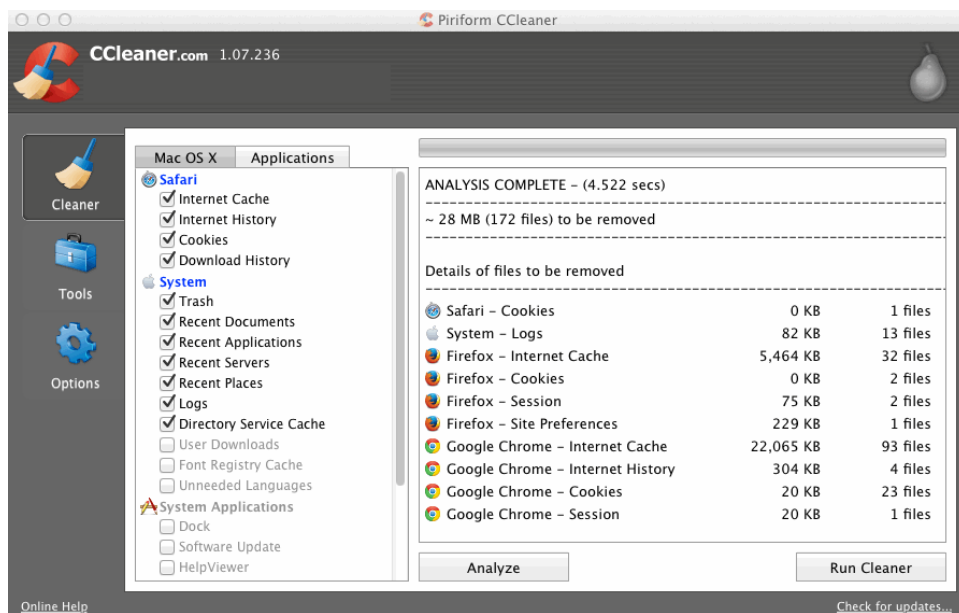
A consideration when running a clean up tool of this sort: be sure you don't accidentally delete log files that you may want or need in the event that a cyber incident occurs. (You need to balance the potential privacy implications of those log files with their potential usefulness in the event that an intrusion takes place).

You can download CCleaner from <http://www.piriform.com/mac>

CLEANUP CACHED FILES

Security	+
Privacy	++
Simplicity	0
Cost	0
Usability	-
Performance	0

Targeted risk: leakage of no-longer needed information



You may also want to consider searching your computer for potential social security numbers or credit card numbers that you may have saved in files and then forgotten about. An example of a free/open source program that will check for this is the Cornell University Spider for OS X, see <http://www2.cit.cornell.edu/security/tools/>

When the Cornell Spider finishes running, be sure to review the log file it produces (normally this will be on your Mac's desktop, unless you change the location for that file in the Spider's preferences).

IV-8. Cover your camera.

While your laptop's camera will normally only go on when you ask it to be used, you should recognize that some hacker/crackers,⁸¹ and some government agencies,^{82,83} have demonstrated the ability to enable your camera without your consent, in some cases doing so without activating the normal "camera on" warning light that's on many cameras.

If you know you will NEVER need to use your integrated Mac camera, you can have an Apple-certified technician remove it, but recall that we assume that you can't intentionally and permanently break your gear.

The next best solution if your laptop has an integrated camera would be to cover it with a piece of opaque black electrical tape if it doesn't have an integrated sliding cover or other physical lens block. You can always remove the tape if you need to use your camera. The rest of the time, it will be "off by default."

The camera on most laptops can be found on/near the top edge of the screen, as shown in the illustration below.⁸⁴



COVER YOUR CAMERA

Security	0
Privacy	+++
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: surreptitious video surveillance of user

⁸¹ <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/>

⁸² <http://www.csmonitor.com/Innovation/Tech/2014/0311/Why-you-should-cover-your-webcam-video>

⁸³ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

⁸⁴ Image credit: http://en.wikipedia.org/wiki/File:MacBook_white.png

IV-9. Mute your microphone.

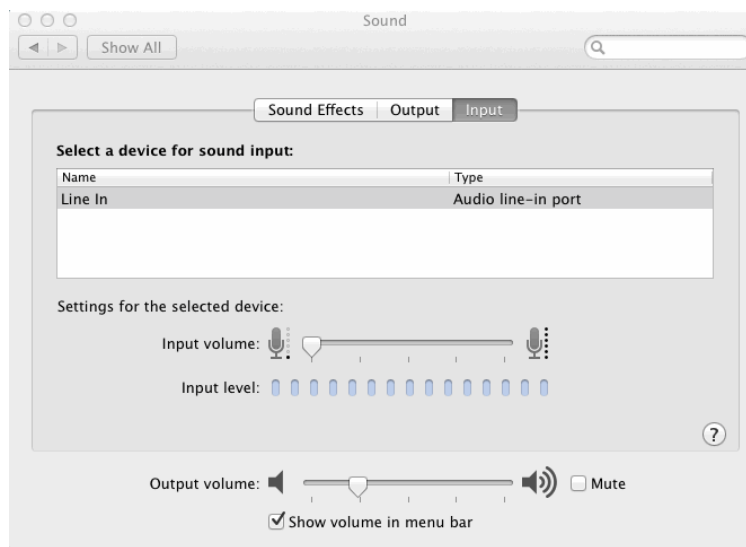
Your system's integrated microphone is also potentially an eavesdropping risk. If you're sure that you'll NEVER need to use your integrated Mac microphone (you can always plug in an external one, right?), you can have an Apple-certified technician remove it, but recall our premise that you can't intentionally and permanently break your gear.

Therefore, just as you taped over your camera, you may also at least want to tape over your Mac's microphone -- that is, if you can successfully locate it (sometimes it can be challenging to do so). Tape won't totally block sound from reaching the microphone, but it may at least muffle some sounds. You should also mute the microphone in software, but be aware that if you can "mute it" in software, you can probably also "unmute it" in software.

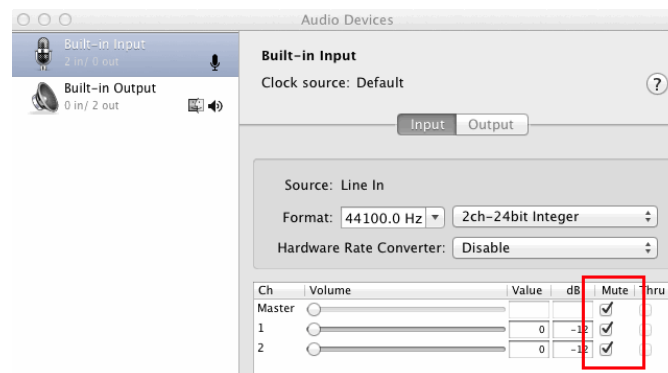
MUTE YOUR MIKE

Security	0
Privacy	++
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: surreptitious audio surveillance of user.



Another option is to selecting a different (non-existent) audio input source. See also /Applications/Utilities/Audio MIDI Setup.app (check all Mute boxes)



The NSA has additional suggestions for dealing with your camera and microphone that they mention in their hardening tips trifold guide.⁸⁵

⁸⁵ http://www.nsa.gov/ia/_files/factsheets/macosex_10_6_hardeningt看ps.pdf

IV-10. Install a privacy filter over your display

If you've ever tried using your computer while traveling or at a meeting, you will quickly learn that many people are irresistibly curious about what's on your screen, and will (sometimes rather rudely) stare at your computer's display.

To deter "shoulder surfing" of this sort, purchase and install a 3M privacy filter.⁸⁶ When installed, these filters make it very difficult for someone sitting beside you to "accidentally" see what's on your screen.

Note that while the 3M privacy filter does a good job of preventing those near you from seeing what's shown on your screen, they may still be able to watch what you type on your keyboard, including things like passwords.⁸⁷

You should also be alert to the possibility that ceiling mounted pan/tilt/zoom security cameras may also be able to easily monitor what you type in some public spaces.

PRIVACY FILTER

Security	0
Privacy	+++
Simplicity	0
Cost	-
Usability	0
Performance	0

Targeted risk: shoulder surfing.

IV-11. What About Using a "Locate My Lost or Stolen Laptop" Program?

A number of programs are available that can be installed and potentially used to help locate a lost or stolen laptop, perhaps providing geolocation information, or allowing you to remotely activate the system's web cam (to see who's using your system), or allowing you to grab a copy of the screen, etc. Those sort of capabilities are obviously hugely potentially useful if you're trying to figure out what's happened to a missing device. On the other hand, if an unauthorized party is able to turn those capabilities against you, obviously this could totally compromise your own privacy.

Some "locate my lost or stolen laptop" programs may also not transmit the information they collect via encrypted channels.

Given those potential realities, we cannot recommend the installation and use of a "locate my lost or stolen laptop" program at this time.

IV-12. Install A Firmware Password?

You have the option of setting a firmware password⁸⁸ on your Mac to prevent things like booting from alternate media, resetting the PRAM on your Mac, etc. We don't necessarily recommend that you do so, however.

Using a firmware password may increase the security of your Mac against a subset of potentially serious attacks, but if you forget your firmware password, you may need to bring your system in to an Apple store to get it reset.

LOST/STOLEN LAPTOP LOCATOR SOFTWARE?

Security	+
Privacy	0/---
Simplicity	0
Cost	0/-
Usability	0
Performance	0

Targeted risk: loss or theft.

⁸⁶ <http://www.3m.com/product/information/Privacy-Computer-Filter.html>

⁸⁷ <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10109460/Edward-Snowden-defence-contractor-gives-up-very-comfortable-life-to-blow-whistle-on-NSA-surveillance-of-Americans.html> included mention of the fact that Edward Snowden would routinely place a large hood over his head and laptop when typing passwords so that any hidden cameras couldn't capture them.

⁸⁸ <http://osxdaily.com/2014/01/06/set-firmware-password-mac/>

V. SECURING ACCOUNT-RELATED ITEMS

V-1. Create a non-admin account for routine use; don't browse from an admin account.

If you do accidentally do something unsafe, the potential impact will usually be less if you're running as a "regular" user rather than a "privileged" user (e.g., administrator, root, etc.) Never casually surf the web or read your email while running as a privileged user.

To create a non-administrative account: System Preferences --> Systems --> Users & Groups --> + (to add a new User).

Be sure the user type is "Standard" and NOT "Administrator."

NON-ADMIN ACCOUNT

Security	++
Privacy	0
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: privilege minimization

New Account: Standard

Full Name:

Account name:

Password:

Verify:

Password hint:
(Recommended)

? Cancel Create User

V-2. Make sure your system's passwords are long, strong, and unique.

Use a mixture of upper and lower case letters, numbers, and special symbols, and a password that's at least 12 characters long.

You can change your login password on your Mac from System Preferences --> Security & Privacy --> General Tab --> Change password.⁸⁹

While you're on that tab, also ensure that "Require password for sleep and screen saver has been set (typically to "after 5 seconds").

Be sure that "Disable automatic login" has also been checked.

Any unused accounts should be removed.

We assume that you will be disciplined enough to force yourself to pick a strong password.

If you're worried you're going to backslide and pick a weak password, you can *force* yourself to use of strong passwords on an unmanaged system (including things like non-reuse of your most recent half-a-dozen passwords and forcing a change of passwords every ninety days). Go to a terminal window and use the commands:

```
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresAlpha=1"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresNumeric=1"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresSymbol=1"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "minChars=12"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "usingHistory=6"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy \
"passwordCannotBeName=1"
$ sudo pwpolicy -n /Local/Default -setglobalpolicy \
"maxMinutesUntilChangePassword=129600"
```

STRONG PASSWORD

Security	++
Privacy	+
Simplicity	0
Cost	0
Usability	-
Performance	0

Targeted risk: password cracking/brute forcing.

⁸⁹ Having trouble picking a strong new password? On some versions of OS X, click the little "key" icon next to the password box for the OS X password assistant -- it will help you pick a strong and usable password, if you're not able to do so spontaneously.

V-3. Ensure that the "root" user in Mac OS X isn't enabled.

The root user is a Unix holdover. If you login as root, you will have full privileges and can basically do anything: you can access/change/delete any file, kill any process, or otherwise do what you please. This is an exceptionally powerful, highly privileged account. Most users don't need to have the root user enabled in OS X.

If you're like most people and DO NOT need to have root enabled, confirm that the "root" use is disabled.

To do so, following Apple's directions for your version of Mac OS X.⁹⁰

NO ROOT USER

Security	++
Privacy	0
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: accountable use of least privilege needed

V-4. Don't "cache" sudo status by default.

The sudo command allows approved users (e.g., Administrator users) to do superuser ("root") tasks.

By default sudo remembers, or "caches," the fact that you've recently sudo'd for five minutes. During that time you won't be asked to enter an administrator password to sudo again. While this is convenient (and will keep you from going nuts) if you're doing a whole series of administrative tasks, this is also a material vulnerability.

To disable that window of time:

```
$ sudo visudo
```

In the Default specification section add the line:

```
Defaults timestamp_timeout=0
```

NO SUDO CACHING

Security	+
Privacy	0
Simplicity	0
Cost	0
Usability	--
Performance	0

Targeted risk: infection of base operating system.

⁹⁰ <http://support.apple.com/kb/ht1528> tells you how to ENABLE root, but you can also use that document to help you DISABLE root (the preferred setting), just make sure that things are set properly when you're done!

V-5. Guest account.

If you're security and privacy conscious, your system is not going to be used for guest access. Therefore, in Systems Preferences --> Users & Groups , click on Guest Account. Allow guests to log in to this computer should be UNCHECKED. Allow guests to connect to shared folders should be UNCHECKED.

NO GUEST ACCOUNT

Security	+
Privacy	0
Simplicity	0
Cost	0
Usability	-
Performance	0

Targeted risk: infection of base operating system.

V-6. Use a password manager/password safe.

Besides your laptop or desktop password, we know that many users have many other passwords that they also need to securely manage. One of the better solutions for managing those is use of an online encrypted password safe. One popular free/open source option for that purpose is KeePass.⁹¹

Other popular password managers include: LastPass,⁹² 1Password,⁹³ mSecure,⁹⁴ etc.

PASSWORD MANAGER

Security	++
Privacy	0
Simplicity	+
Cost	0/-
Usability	+
Performance	-

Targeted risk: use of weak passwords/same passwords

⁹¹ <http://keepass.info/>

⁹² <https://lastpass.com/>

⁹³ <https://agilebits.com/onepassword>

⁹⁴ https://msevensoftware.com/msecure_mac

VI. SECURING LOGIN-WINDOW-RELATED ITEMS

VI-1. Configure the system login preferences for security

There are steps you can take to minimize the attack surface you present to someone who has physical access to your laptop.

In Systems Preferences --> Users & Groups --> Login Options make sure that:

-- Automatic login: Off

-- Display login window as: Name and password

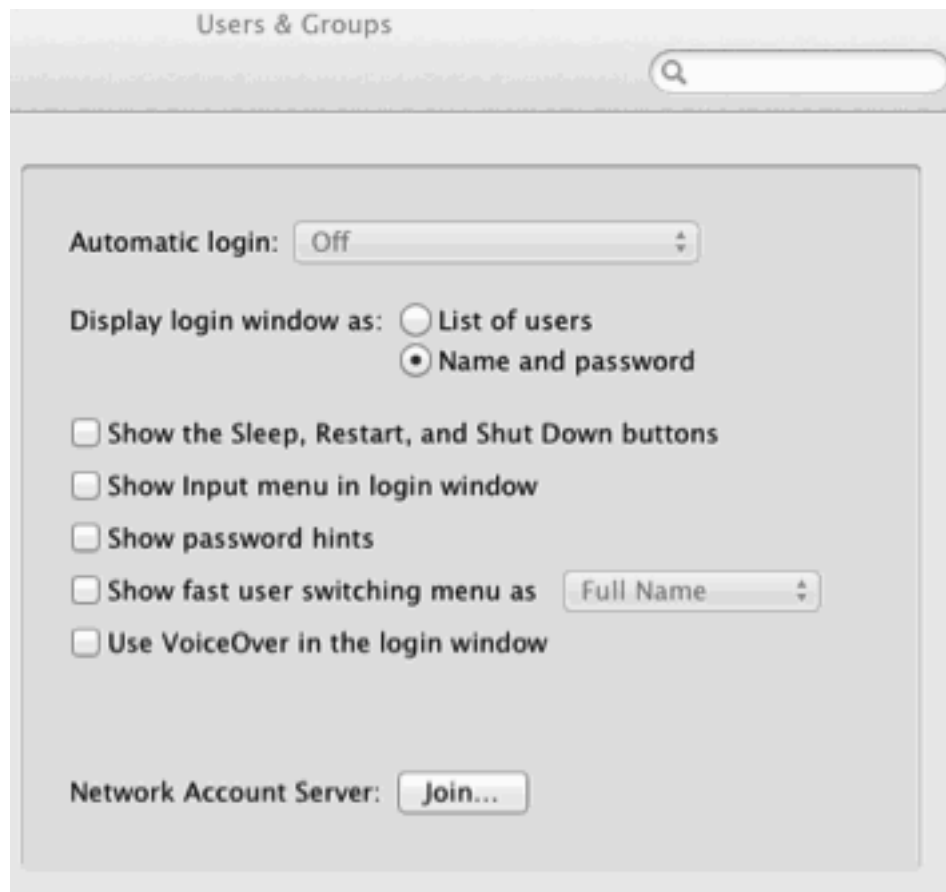
All other check box options should NOT be checked.

Network Account Server -- if you click Join, you normally shouldn't see a server listed.

LOGIN WINDOW CONFIG

Security	+
Privacy	+
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: info leakage to user with console access



VI-2. Warning banners

While we're working on the login screen, let's also add a basic warning banner forbidding unauthorized access.

Although addition of this banner does nothing (technically) to prevent unauthorized access, the presence of a warning banner may make some prosecutors more comfortable proceeding when it comes to establishing that an intruder knew or should have known that they weren't welcome....⁹⁵

In a terminal window, enter:

```
% sudo defaults write \
/Library/Preferences/com.apple.loginwindow LoginwindowText \
"Unauthorized Access Forbidden"
```

The exact language preferred or required for your location may vary.

Assuming you also allow ssh remote logins, be sure to also add that same banner to the sshd config. To do so, use vi or your favorite editor to create a file containing the banner you want to use:

```
$ sudo vi /etc/sshd-banner
i
Unauthorized Access Forbidden
<ESC>
:wq
$ sudo chmod a+r /etc/sshd-banner
```

Now make sure that the Banner line in your sshd config file (often /etc/sshd_config) is uncommented and points at the new sshd-banner file you've just created. Try ssh'ing into your own system to confirm that the new warning banner works as expected.

WARNING BANNERS

Security	+
Privacy	0
Simplicity	0
Cost	0
Usability	0
Performance	0

**Targeted risk: potential
impediments to prosecution**

⁹⁵ See for example "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> at PDF page 170.

VI-3. Activate Active Screen Corners for locking your screen

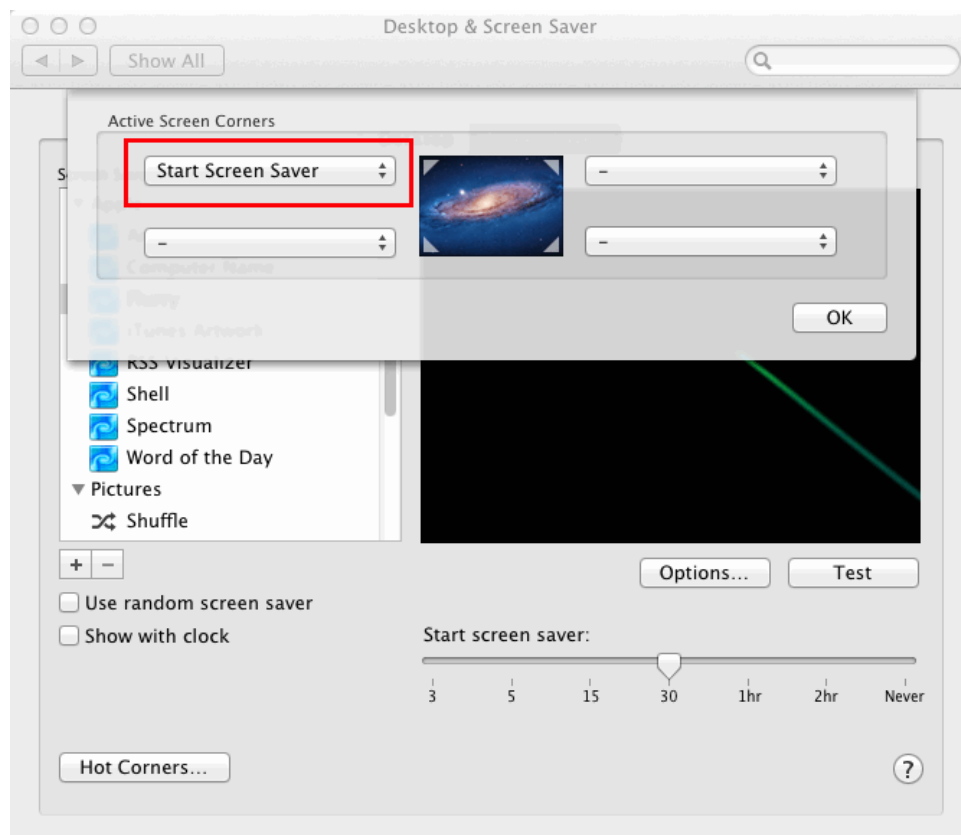
When you step away from your system, it's a good idea to always lock your screen. To do so,

System Preferences --> Mission Control --> Hot Corners... --> Start Screen Saver (for at least one corner)

MANUAL SCREEN LOCK

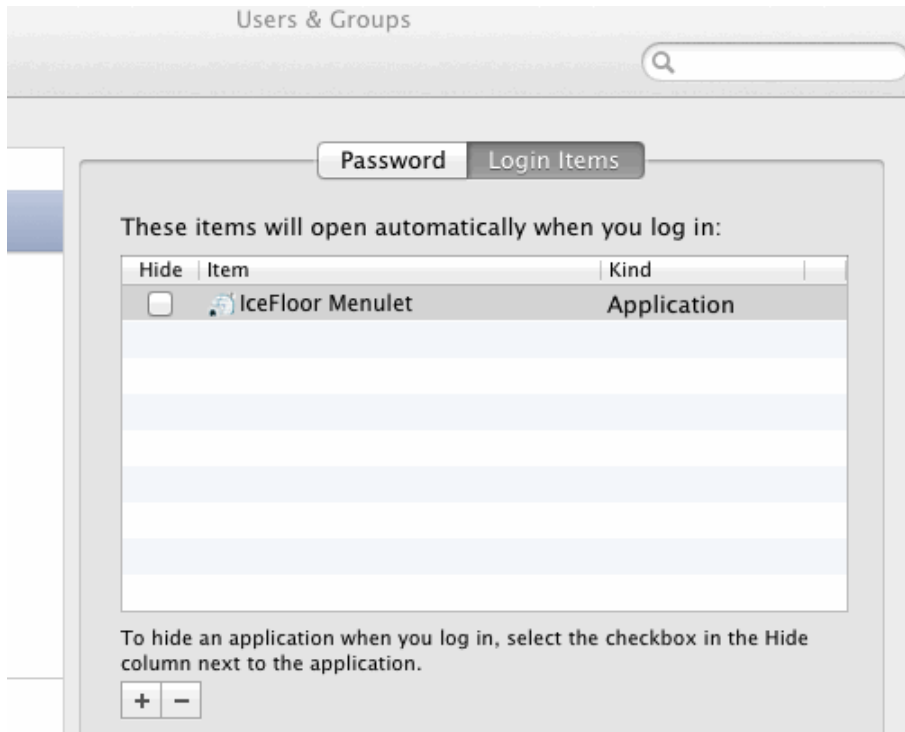
Security	+
Privacy	+
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: local access to unlocked logged in user acct



VI-4. Review and Disable Any Unneeded Login-Time/Boot-Time Automatically-Launched Items

For Login-Time items, start by checking System Preferences --> Users & Groups --> Login Items Tab. For example, you may see "iTunesHelper" enabled. Unless you routinely use the associated application, you can disable unneeded items by highlighting each item and then clicking the minus sign. In this example, we only have one automatically launched item, the IceFloor firewall menulet.

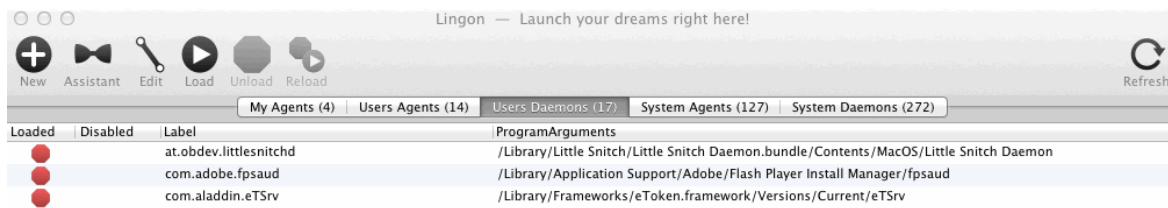


AUTO-LAUNCHED ITEMS

Security	++
Privacy	0
Simplicity	+
Cost	0
Usability	0
Performance	+

Targeted risk: unneeded auto-launched services

Additional programs (not shown in the LoginItems preferences panel) may also be run at boot time, or at user login. You may notice these when you see them attempting to communicate outbound, if you're running Little Snitch. The easiest way to review and manage these is probably via the program "Lingon."⁹⁶



Disable applications in Lingon with care, particularly when it comes to System applications. You can render your system unstable (or even unbootable) if you randomly disable critical functionality, so proceed carefully and **ensure that your system is fully backed up before making any changes in this area.**

⁹⁶ <http://www.peterborgapps.com/lingon/> (nominal fee applies) or <http://sourceforge.net/projects/lingon/>

VII. CONFIGURING NETWORK CONNECTIVITY

VII-1. Disable all unneeded network interfaces.

For example, if you only connect via Ethernet, disable Bluetooth, Wi-Fi, and FireWire network interfaces.

On the other hand, if you only connect via Wi-Fi, disable all the other network interfaces.

To do this, go to System Preferences --> Network and confirm that only the appropriate network interface is green, and all the others are red.

If you have more than one location defined, review and adjust the network interfaces that are shown as live for EACH location.

NETWORK INTERFACES

Security	+
Privacy	0
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: unused ints = increased attack surface

VII-2. Review and adjust network connectivity settings as appropriate.

Do this from System Preferences --> Network --> Advanced (after you've clicked on Ethernet or Wi-Fi, as appropriate):

TCP/IP Tab:

-- *Configure IPv4*: In most cases, leave this tab alone.

-- *Configure IPv6*: If IPv6 is locally available, set to "Automatically."

If allowed by your local network's policies, enable use of IPv6 privacy extension addresses by going to a terminal window (see /Applications/Utilities/Terminal.app) and entering:

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=1
```

NET CONFIGURATION

Security	+
Privacy	+
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: Windows networking; IPv6 addresses

DNS Tab:

-- In most cases, leave this tab alone, too.

Note: *DNS represents another potential avenue by which you may end up being monitored.*

That is, when you visit the site www.example.com, your computer uses the domain name system (DNS) to translate that fully qualified domain name (FQDN) to a numeric IP address.

The DNS infrastructure (typically your network connectivity provider's recursive resolver) that does that translation may potentially log those domain names, and the source of those queries (e.g., the IP address of your network connection).

For example, if you visit job listing sites from your employer's connectivity, the administrator of your employer's DNS server may be able to see that you're potentially looking for a different job from your work computer.

Option: some ISPs or other connectivity providers may allow you to specify alternative name servers.

Important Privacy Warning: If you elect to use alternative name servers, *be sure to understand the privacy policy associated with those alternative name servers. In some cases the privacy of alternative name servers may be better -- or WORSE -- than the privacy of your default name servers.*

Important Security Warning: If you use an untrustworthy alternative DNS server, you may be taken to a fake site pretending to be your bank, broker, popular online retailer, etc.

Important Content Filtering Warning: Some publicly available alternative DNS servers may intentionally filter some categories of content including known or suspect malware-related sites, phishing sites, adult content, violent sites, etc. Ensure that the name servers you decide to use have a content filtering policy you agree with.

A few lists of intentionally publicly available DNS servers can be found at:

-- <http://pcsupport.about.com/od/tipstricks/a/free-public-dns-servers.htm>
 -- <https://www.grc.com/dns/alternatives.htm>
 -- http://www.wikileaks.org/wiki/Alternative_DNS

WINS Tab:

-- If you don't use WINS/NetBIOS (aka "Windows Networking"), disable it. Typically you will be able to do this by opening a Terminal window and entering the command:

```
sudo launchctl unload -w \
/System/Library/LaunchDaemons/com.apple.netbiosd.plist
```

You'll need to know the admin password for your Mac to sudo; in some cases, you may need to tweak the location of the plist file from the typical value shown above.

If You've Made Changes to ANY of the Above Network Preferences...

When done configuring Network preferences, click OK/Apply to save any changes. If you have multiple profiles, you'll want to review and update EACH of your profiles.

DNS CONFIGURATION

Security	+/-
Privacy	+/-
Simplicity	-
Cost	0
Usability	+/-
Performance	0

Targeted risk: Windows networking; IPv6 addresses

VII-3. Connect directly, not via a local/enterprise proxy server

Some sites send all local web traffic through a "web cache" or "proxy server." These devices can be commercial devices,⁹⁷ or built from free/open source software such as Squid,⁹⁸ and they can serve multiple purposes, including:

- caching frequently used content that rarely changes, thereby avoiding the need to repeatedly download the same file time after time after time
- improving throughput by serving files locally, thereby reducing latency and driving down bandwidth-delay product values
- proxy servers can also scan web traffic for malicious software, or block access to unauthorized categories of content

While blocking malicious software or improving performance or reducing wide area congestion all sound like terrific objectives, web cache servers can *also* represent a potential point at which privacy may get compromised, since most web cache servers log the traffic that passes through them, and administrators may review (or be compelled to produce) those logs.

Thus, as a general rule, privacy conscious users will NOT want their traffic to go via a local web cache or local proxy server.

Avoiding this may range from trivially easy to quite difficult, depending on how the local web cache or proxy server has been configured. You may want to begin by checking to see if there are indications that your connection is using a proxy server. One way to do so is by visiting:

<http://www.lagado.com/proxy-test>

If that site reports that you are connecting via a proxy server, you can attempt to disable use of the local proxy server, as described on the next page...

LOCAL PROXY SERVER	
Security	-
Privacy	++
Simplicity	+
Cost	0
Usability	+
Performance	-
Targeted risk: potential local content monitoring	

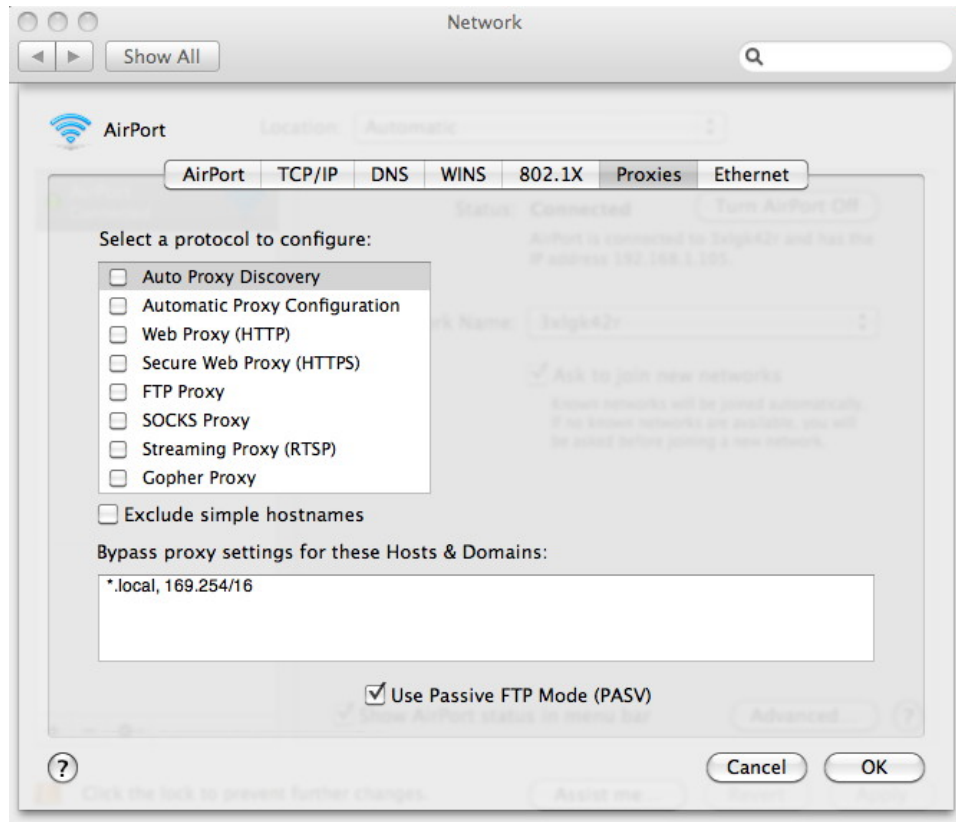
⁹⁷ For example, see <http://www.bluecoat.com/products/cache-flow> or <http://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html>

⁹⁸ <http://www.squid-cache.org/>

Attempting to Opt-Out of Caching

Apple Menu --> Systems Preferences --> Network --> Advanced --> Proxies tab.

Ensure all protocols are UNCHECKED. Click OK, and then click Apply.



Note that if your local network requires you to use a proxy server to access the Internet, disabling use of that proxy server will break your access to the Internet.

Also note that even if you attempt to opt out as shown above, your traffic may still be involuntarily routed through a caching appliance under some circumstances. After attempting to "opt-out" confirm that you've actually successfully done so.

VII-4. Use a 3rd Party VPN?

Depending on your circumstances, you may want to consider using a 3rd Party VPN to protect your network traffic from local network monitoring.

To be clear about this issue, here's the risk to your privacy if you *don't* use an off site VPN: local network engineers or security staff, if they are monitoring your traffic, can see the sites to which you're connecting. If you're using a third party VPN, a local network engineer can see that you're connecting to that VPN, but cannot see what's inside of that encrypted VPN tunnel.

3RD PARTY VPN?

Security	--
Privacy	++/--
Simplicity	-
Cost	--
Usability	-
Performance	-

Targeted risk: potential local network monitoring

If you *do* decide to use a VPN, pick your VPN provider carefully:

while you'll be getting protection from potential local snooping by routing your traffic through that VPN, if you pick an untrustworthy VPN service (or a VPN service that happens to have been targeted for external monitoring), you may trade a reduction in *local monitoring* for an increased risk of *remote monitoring* (e.g., by your VPN provider, or by a government agency targeting that provider). That may not such a great trade, shall we say. There are a few other considerations you should keep in mind when selecting a VPN provider:

-- One consideration is where your VPN provider is located. Some locations require more in the way of logging than other parts of the world. Some locations are more difficult for the authorities to serve legal paperwork on than others. Still other locations may have strong(er) privacy laws.

-- Most legitimate VPN services charge a monthly (or yearly) fee. Beware of any VPN service that doesn't. Of course, paying for VPN service with a credit card or other traditional payment channel may link your identity to your VPN traffic. You may want to look for a provider that accepts a more anonymous payment option, such as some online currencies, or cash.

-- A VPN provider may routinely log what you do (although there are services that claim they don't/won't do so, or will only do so on a minimal and short term basis). You may at least want to investigate what logging policy the provider claims to follow.

A review of some anonymity-oriented VPN services can be found at:

-- "Which VPN Services Take Your Anonymity Seriously? 2013 / 2014"

<http://torrentfreak.com/vpn-services-that-take-your-anonymity-seriously-2013-edition/>

Whether you decide to trust *any* VPN service is a decision that only you can make.

VII-5. Use Tor?

Another option, if you're worried about local monitoring, would be to use Tor.⁹⁹ Sites that are prone toward draconian monitoring policies may locally "outlaw Tor," so that the sheer act of connecting to a Tor node may be considered a violation of local policy. (This may not be true for connections via your local commercial ISP from home, etc., check your terms of service carefully)

TOR?

Security	0
Privacy	++/--
Simplicity	-
Cost	0
Usability	-
Performance	--

Targeted risk: potential local network monitoring

⁹⁹ <https://www.torproject.org/>

VIII. OTHER SYSTEM PREFERENCE AND MISCELLANEOUS TWEAKS

VIII-1. *Confirm that sharing is disabled.*

See System Preferences --> Sharing. Everything should be unchecked (unless you want to be able to ssh into your system, in which case enable remote login)

SHARING

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: unintentional access to system/files

VIII-2. *Ensure O/S privacy settings are appropriate.*

On the Mac, go to System Preferences --> Security & Privacy --> Privacy Tab, then ensure that "Send diagnostic & usage data to Apple" is unchecked, and that "Enable Location Services" is also unchecked.

O/S PRIVACY

Security	0
Privacy	+
Simplicity	0
Cost	0
Usability	-
Performance	0

Targeted risk: leakage of system usage/location info

VIII-3. *Ensure that Date & Time are NOT set to "set time and time zone automatically"*

Go to the System Preferences --> Date & Time --> Date and Time Tab. Make sure "Set date and time automatically" isn't checked. Once you've done so you'll need to manually ensure that your system's clock remains synced and sane. See System Preferences --> Date & Time --> Time Zone Tab. Make sure "Set time zone automatically using current location" is disabled.

DATE/TIME SETTINGS

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

Targeted risk: leakage of hints about system location

VIII-4. Eliminate "Recent" Items:

Systems Preferences --> Appearance , then set all the "Recent Items" to "None"

You may also want to try using OnyX¹⁰⁰ to suppress Open Recent Item display (see Parameters --> General tab in that program)

RECENT ITEMS

Security	0
Privacy	+
Simplicity	0
Cost	0
Usability	-
Performance	0

Targeted risk: leakage of app usage information

VIII-5. Print Jobs: Disable List of Print Jobs.

In the terminal window, enter:

```
$ cupsctl PreserveJobHistory=No
```

PRINT JOB LISTING

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

Targeted risk: leakage of system usage information

VIII-6. Clear shell history in terminal.

When you enter commands in a terminal shell window, the commands you enter get remembered by default in the bash history file. To clear those commands, open a terminal window and enter:

```
$ history -c
```

Check the shell history by entering:

```
$ history
```

SHELL HISTORY

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

Targeted risk: leakage of system usage information

¹⁰⁰ <http://www.titanium.free.fr/downloadonyx.php>

VIII-7. Confirm that user home directories aren't group or world readable or traversable.

For each home directory in the /Users directory, enter the command:

```
$ sudo chmod go-rx /Users/username
```

where "username" in that command is actually the name of a user's directory.

FILE PROTECTIONS

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: unintentional information disclosure

VIII-8. Disable the Spotlight local search engine.

In general, Spotlight attempts to index everything.

Disable it by saying:

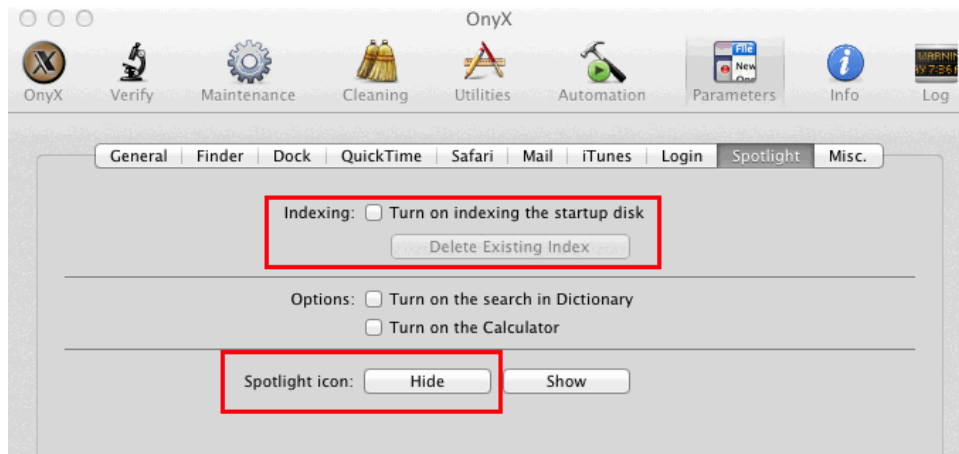
```
$ sudo mdutil -a -i off
$ sudo launchctl unload -w \
/System/Library/LaunchDaemons/com.apple.metadata.mds.plist
```

LOCAL SEARCH ENGINE

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	-

Targeted risk: unintentional information disclosure

You may also want to hide the Spotlight icon in your toolbar. An easy way to do that is with OnyX:¹⁰¹ in Onxy --> Parameters --> Spotlight --> Spotlight Icon: Hide



You may also want to delete any already-created Spotlight search files living in the /.Spotlight-V100 directory (and any .Spotlight-V100 files living in the root directory of any other mounted filesystems)

¹⁰¹ <http://www.titanium.free.fr/downloadonyx.php>

VIII-9. Securely delete any files in the trash.

When you delete files on a Mac, files are unlinked in a way that leaves them potentially vulnerable to being forensically recovered. To *securely* delete files that have been put in the Mac trash can, begin using Finder --> Secure Empty Trash...

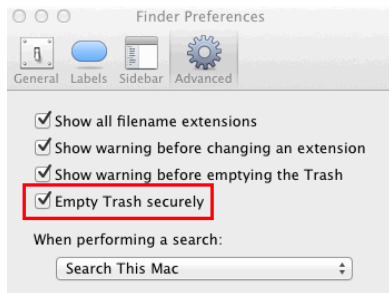
To set this as the default, go to Finder --> Preferences --> Advanced --> Empty Trash Securely

While you're there, also ensure that Show all filename extensions is also checked.

SECURE FILE DELETION

Security	+
Privacy	++
Simplicity	0
Cost	0
Usability	-
Performance	-

Targeted risk: forensic recovery of "deleted" files



To securely delete files at the *command line prompt* (e.g., in a terminal window), use the *srm* command instead of the normal *rm* command.

IX. LEARNING MORE ABOUT SECURING MAC OS X

IX-1. Additional Mac operating system security/privacy reading.

While the preceding may feel painfully long already, we're really just scratching the surface. For a more detailed treatment, see:

- "Mac OS X Security Configuration Guides," <https://ssl.apple.com/support/security/guides/>
(note: unfortunately, the most recent version of Mac OS X documented here is Mac OS X v10.6 (Snow Leopard), and you should NOT run an old version of Mac OS X if you can possibly avoid it!)
- "Mac Common Criteria Configuration and Administration Guide," [dated 2009; another 10.6-era document], <https://ssl.apple.com/support/security/commoncriteria/CommonCriteriaAdminGuide.pdf>
- "Mac OS X Checklist 1.1," <http://www.sans.org/score/macosexchecklist.php>
(note: unfortunately, this document dating from 10/26/2008 targets OS X v10.5, an even older release!)
- "OS X Hardening: Securing a Large Global Mac Fleet,"
https://www.usenix.org/sites/default/files/conference/protected-files/castle_lisa13_slides.pdf (enterprise oriented, security (rather than privacy) focused)
- "CIS Apple OSX 10.8 Benchmark v1.0.0"
<https://benchmarks.cisecurity.org/downloads/form/index.cfm?download=osx108.100>
- DoD Security Technical Implementation Guides (STIGS), including for the Mac
<http://www.stigviewer.com/stigs>

Books:

"Practical Paranoia: OS X Security Essentials for Home and Business: The easy step-by-step guide to hardening your OS X security," Marc L. Mintz, July 2013, ISBN: 978-1490458380.

IX-2. Subscribe to the Apple security announcement mailing list.

<https://lists.apple.com/mailman/listinfo/security-announce>

X. SECURING THE WEB BROWSER (FINALLY!)

X-1. Picking The "Most Secure" Browser

There are many different browsers that you could choose to run. Some users (potentially including you!), may just run the browser comes with their operating system, e.g., Safari in the case of Macs.

However, increasingly, many users choose to run an alternative browser, such as Chrome, Firefox, or Opera, instead.

Given that your choice of browsers is one of the most basic of all web browser security and privacy-related questions, ***how should you decide which browser to run?***

Here are some factors you may want to consider (there may be additional factors that are also relevant).

a. Unpatched Vulnerabilities? Are Only Old Versions Available For My System? Secunia provides summary statistics about security vulnerabilities in many software products, including web browsers.¹⁰² *At the time this document was written*, all of the following browsers had zero unpatched vulnerabilities:

-- Apple Safari (7.x):¹⁰³

-- Google Chrome (34.x):¹⁰⁴

-- Mozilla Firefox (28.x),¹⁰⁵ and

-- Opera Software Opera (20.x)¹⁰⁶

This may change by the time you're reading this, later, but at least at this snapshot in time, the *latest version* of all popular browsers for the Mac are (technically) "equally secure" when it comes to unpatched vulnerabilities. That's good, as far as it goes.

Unfortunately, in at least some cases, the most recent version of popular browsers may not be available for all operating system.

For example, only dated versions of Safari are currently available for some older versions of Mac OS.¹⁰⁷ Likewise, while Safari is available for MS Windows, the latest version of Safari available for that operating system is 5.1.7, while the current version of Safari (as used in "Mavericks" (OS X 10.9.1) is version 7.0.1. *Implicitly, this means that there may be unpatched vulnerabilities in the best available version of Safari on some platforms.*

¹⁰² <http://secunia.com/community/advisories/>

¹⁰³ <http://secunia.com/advisories/product/48957/>

¹⁰⁴ <http://secunia.com/advisories/product/49957/>

¹⁰⁵ <http://secunia.com/advisories/product/49761/>

¹⁰⁶ <http://secunia.com/advisories/product/49650/>

¹⁰⁷ <http://support.apple.com/downloads/#safari>

b. Some Platforms May Not Be Able to Run A Particular Browser At All. For example, MS Internet Explorer isn't available for the Mac. This rules out MS Internet Explorer for the purposes of this Mac-focused document.

c. Avoid Obscure Browsers. Given that we assume that you care about privacy as well as security, don't run an uncommon browser. Why? Doing so would, in and of itself, make you "stand out" from other users, sort of like being the only guy to drive a Model T in your city. For instance, you probably wouldn't want to run the relatively uncommon command line browser Lynx....

d. Avoid Beta (and Alpha!) Versions of Browsers. While it's terrific if you're willing to help test beta (and even alpha!) versions of web browsers, that is another example of an uncommon behavior. Alpha and beta versions of browsers also expose you to bugs that aren't present in more thoroughly tested versions. Beta and alpha versions of browsers may also be more heavily instrumented than production versions of the same browsers, reporting bug info to developers to help them fix code issues or performance problems. Therefore, avoid beta and alpha versions of browsers if you're privacy and security conscious -- let someone else test those builds.

Thus, for example, you should NOT run Firefox Beta¹⁰⁸ or Firefox Aurora,¹⁰⁹ even if you think they sound sort of cool and you'd like to help.

e. You Should Avoid Browsers That Are No Longer Being Actively Developed. For example Camino is no longer being actively developed,¹¹⁰ so you should not use it.

f. Decide If Browsers Developed Abroad Are a Concern For You. For example, while Maxthon is one of the browsers listed at http://www.browserchoice.eu/BrowserChoice/browserchoice_en.htm, and has generally received positive reviews,¹¹¹ it was developed by a company that's based in China.

That may be a source of concern to some security- and privacy-aware Americans, just as use of American software products may increasingly be a source of concern to some users abroad.

¹⁰⁸ <http://www.mozilla.org/en-US/firefox/channel/#beta>

¹⁰⁹ <http://www.mozilla.org/en-US/firefox/channel/#aurora>

¹¹⁰ <http://caminobrowser.org/>

¹¹¹ <http://www.maxthon.com/awards/>

X-2. What's LEFT As A Possible Browser Option?

It might seem as if we've ruled out "everything," but that's not actually the case. Here's your remaining options, from our point of view:

-- **Google Chrome:** This is an exceptionally popular alternative web browser, with over 40% of the market in the US according to some statistics.¹¹²

Google Chrome does some things very right:

- It is generally noted as being particularly fast relative to other browsers.
- It uses sandboxing to limit the security impact of malicious code.
- It integrates Flash (as PepperFlash) and a built in PDF reader as part of the browser (and thus can better avoid vulnerable/unpatched versions of Flash and PDF helper applications).
- It supports TLS 1.2

On the other hand, Chrome has some privacy-related issues:

- Google is a search provider as well as a browser vendor (much as Microsoft is with Internet Explorer and Bing).
- Google Chrome is produced by an organization that "lives or dies" on its online advertising revenues. It finally adopted/implemented the FTC-recommended "Do Not Track" feature, but left it off by default while hiding that option in an obscure location -- that's not in the best interest of users.
- Google Chrome's Safe Browsing technology (if enabled) potentially leaks information about the sites you visit with Google.¹¹³

Chrome also has some default privacy-related practices that make me reluctant to recommend it for security- and privacy-conscious users at this time.¹¹⁴

-- **Mozilla Firefox:** The historic challenger to Internet Explorer and Safari, Mozilla Firefox now has roughly half the market share that Google Chrome has. Many remark on the number of extensions available for Mozilla Firefox, including many popular security and privacy extensions.

Mozilla Firefox is also the browser of choice for security and privacy conscious users in polls.¹¹⁵

Mozilla Firefox's primary drawback is that when both IPv4 and IPv6 are available, Firefox defaults to IPv4 rather than using IPv6.

¹¹² http://en.wikipedia.org/wiki/Usage_share_of_web_browsers

¹¹³ <https://support.google.com/chrome/answer/99020>

¹¹⁴ To Google's credit, they have an excellent privacy web paper -- if people bother to read it. See <https://www.google.com/intl/en/chrome/browser/privacy/whitepaper.html>

¹¹⁵ "Firefox burns Chrome in our trustworthy browser poll," <http://nakedsecurity.sophos.com/2013/09/23/firefox-burns-chrome-in-our-trustworthy-browser-poll/>

-- **Safari:** Safari usage is about half that of Firefox.

There are some recent fixes to Safari security bugs that have given me pause about currently recommending Safari,¹¹⁶ likewise some privacy issues that have emerged.¹¹⁷

-- **Opera:** Opera is the final "mainstream" alternative browser, but Opera is used by just a percent or two of all users. We believe that's too obscure/too distinctive for privacy conscious users.

For the purposes of this document, we recommend (and will document) use of Mozilla Firefox.

At a later date, we may also document use of other browsers.

¹¹⁶ "Apple updates Mavericks to 10.9.1, issues security fixes for Safari,"
<http://nakedsecurity.sophos.com/2013/12/17/apple-updates-mavericks-to-10-9-1-issues-security-fixes-for-safari/>

¹¹⁷ "Google to pay \$17M settlement for bypassing Apple's Safari security settings,"
appleinsider.com/articles/13/11/18/google-to-pay-17m-settlement-for-bypassing-apples-safari-security-settings

X-3. Review Browser Privacy Policies. Many browsers (and most of the web sites that you visit with them!) have privacy policies that talk about how they work, including things like personalization of the browser with a unique "installation number," a characteristic that may potentially allow you to be tracked. Therefore:

PLEASE READ THE PRIVACY POLICY THAT APPLIES TO THE BROWSER YOU'LL BE USING! REALLY! THIS IS IMPORTANT!

Firefox,¹¹⁸ has a browser-specific privacy policy plus additional privacy policies that apply to specific optional features of the browser environment. If your browser uses a multipart privacy policy, review ALL parts of that privacy policy that may apply.

To view the Firefox privacy policy, go to Firefox --> About Firefox --> Privacy Policy:



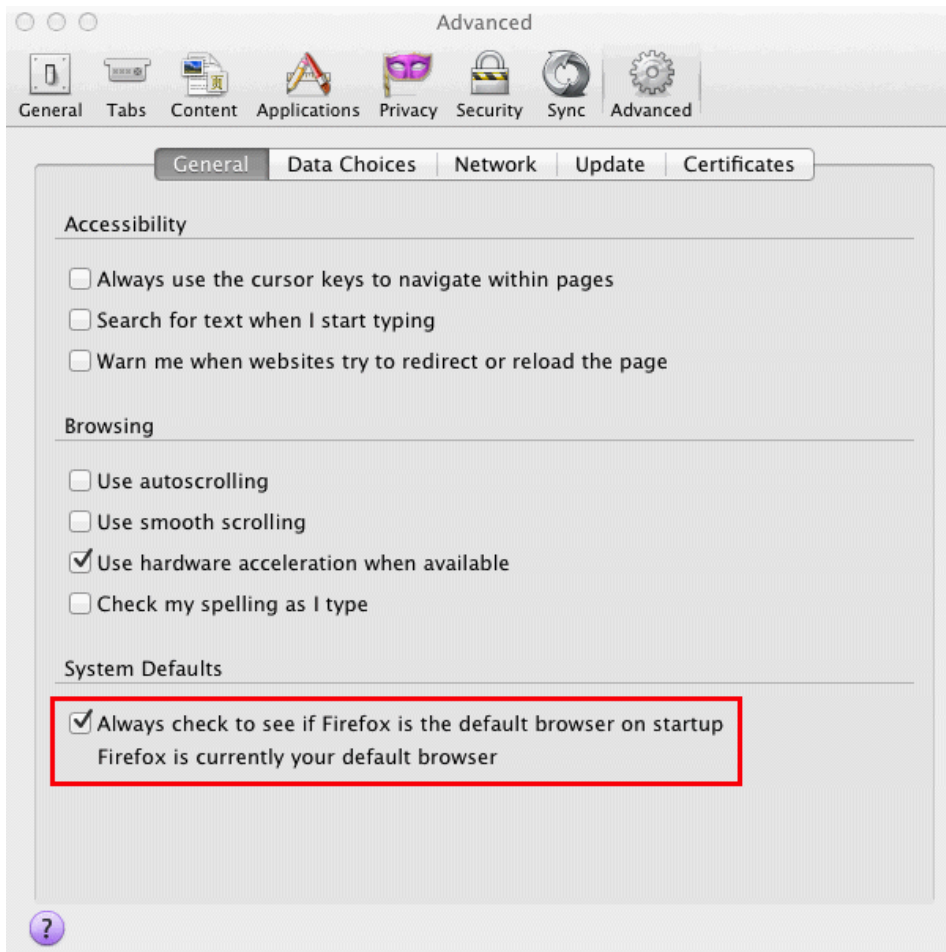
Helpful resource for some major Internet sites: "Terms of Service, Didn't Read:" <http://tosdr.org/>

¹¹⁸ <http://www.mozilla.org/en-US/legal/privacy/firefox> and <http://blog.mozilla.org/addons/how-to-opt-out-of-add-on-metadata-updates/>

X-4. Check to make sure that Firefox is the default browser on startup.

To do this:

Firefox --> Preferences --> Advanced --> General --> System Defaults -->
Always check to see if Firefox is the default browser on startup. See the following illustration:



DEFAULT BROWSER

Security	+
Privacy	+
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: inadvertent use of some other browser

X-5. Keeping Firefox Patched Up-to-Date

Firefox --> Preferences --> Advanced --> Update --> Automatically install updates

While on the same screen, ensure that "Warn me if this will disable any of my add-ons"

If you like, while on this panel, also enable "Automatically update: search engines"

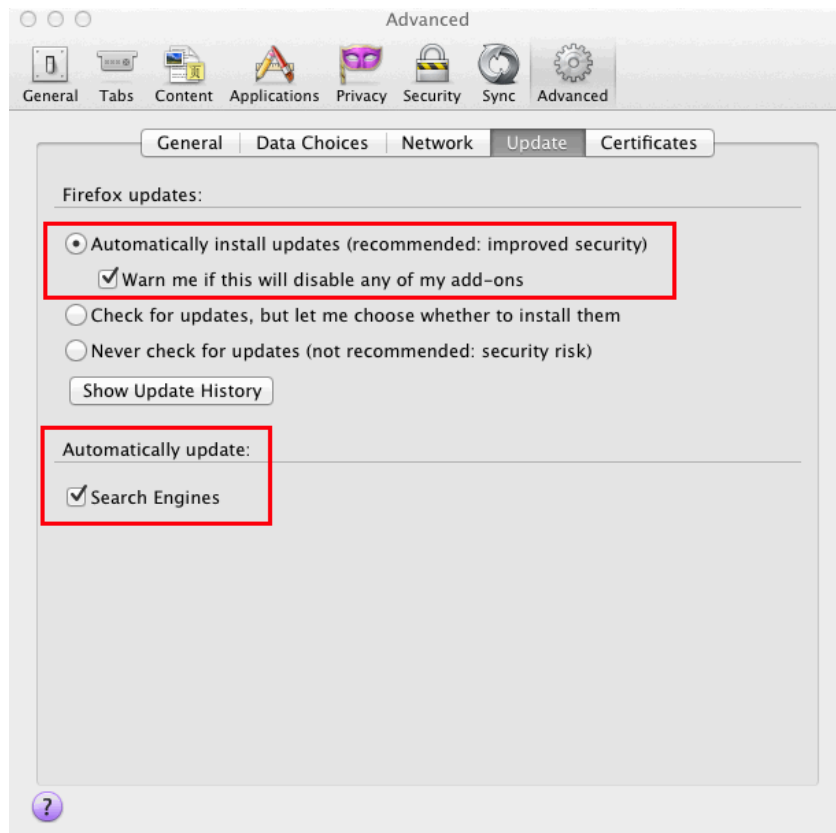
Confirm that Firefox is currently up-to-date by going to Firefox --> About Firefox.

Note that if a new version is available, you will need to restart Firefox after it is updated.

BROWSER UPDATES

Security	++
Privacy	-
Simplicity	0
Cost	0
Usability	0
Performance	0

Targeted risk: inadvertent use of some other browser



X-6. Plugins/Browser Extensions

Firefox's base functionality can be extended with a variety of plugins and browser extensions. Because of the range of plugins and extensions that are available for Firefox it is hard to make a definitive statement about their potential impact on security, privacy, simplicity, cost, usability and performance. Some may help, others may hurt, each of those areas or some combination thereof.

One general statement: plugins and extensions that you don't need/use should be disabled and/or removed to reduce your system's attack surface, and any plugins or extensions you keep should be kept up to date.

You can see the plugins and browser extensions you have installed by going to:

Firefox --> Tools --> Add-ons

Extensions can be disabled and/or removed from the Extensions tab.

Plugins are generally installed in either /Library/Internet Plug-Ins or ~/Library/Internet Plug-Ins and may need to be removed manually.

CAUTION: There are some plugins you shouldn't remove! A list of plugins you should NOT remove can be seen at: <http://support.apple.com/kb/TS3230>

BROWSER PLUGINS

Security	+/0/-
Privacy	+/0/-
Simplicity	+/0/-
Cost	+/0/-
Usability	+/0/-
Performance	+/0/-

Targeted risk: inadvertent use of some other browser

X-7. *Recommended browser plugins/extensions.*

While you generally want to minimize the number of add-ons you install, there are some add-ons that are worth including even if you normally don't use add-ons, including...

X-8. *AdBlock Plus:*

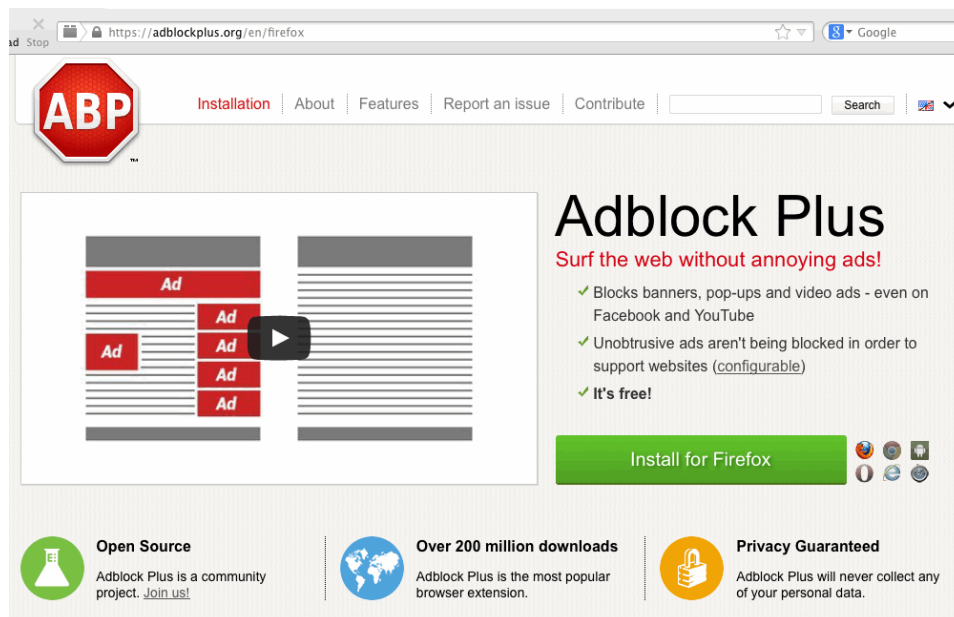
Block annoying advertisements. Advertisements often include trackers, and can serve as a vehicle for dropping malware. You don't need advertisements, so block them. One of the best tools for this is Adblock Plus.

See <https://adblockplus.org/en/firefox>

ADBLOCK PLUS

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

**Targeted risks: malvertising,
user tracking**



Note that Adblock Plus allows some "acceptable ads" by default. If you hate all ads, be sure to click on the Adblock Plus icon, choose Filter Preferences from the menu, and uncheck "Allow non-intrusive advertising."

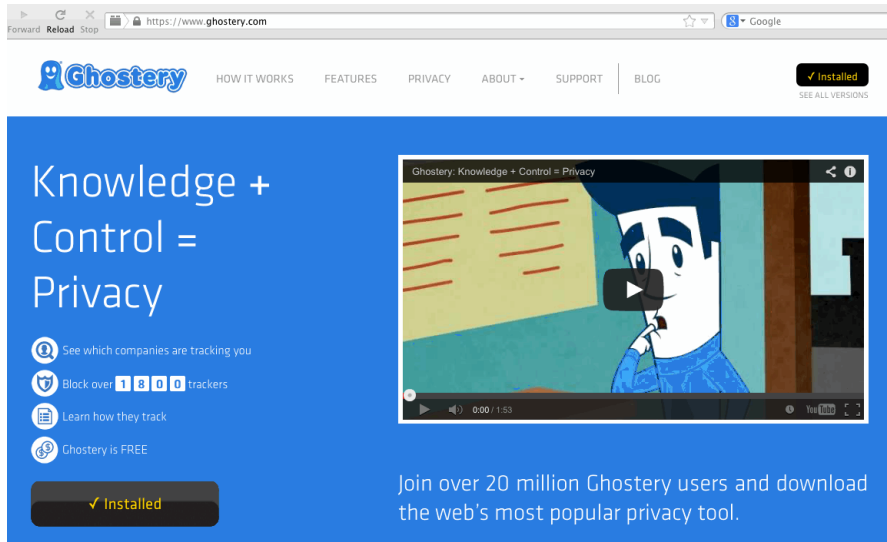
You may also want to consider adding a custom rule to block even Google's sponsored links from showing as part of Google search results (assuming you use Google for your search engine); you can see the custom rule code needed to do this at:

<https://adblockplus.org/forum/viewtopic.php?t=274>

Look for the posting from ecjs at Sun Feb 05, 2006 12:55 pm and add that to Adblock Plus Filter Preferences Custom filter rules.

X-9. Ghostery:

This add on blocks many attempts at tracking you online.
See <http://www.ghostery.com/>



GHOSTERY

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

Targeted risk: user tracking

Be sure to configure Ghostery's General options to:

- Enable tracker library auto-updating
- Under "Blocking Options" choose "select all" for both the Trackers tab and the Cookies tab

Under the Advanced tab:

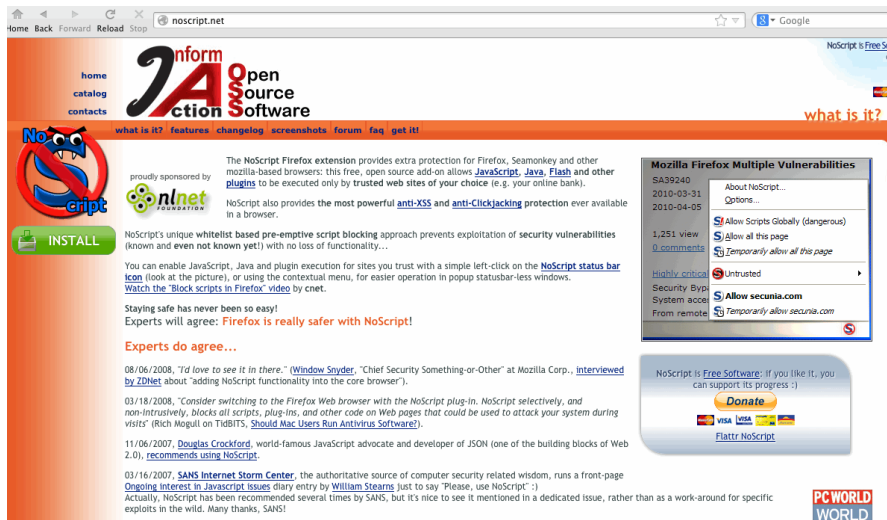
- In the "Auto Update" section, select "Block new elements by default."

We strongly recommend that privacy conscious users NOT send telemetry back to Ghostery about the sites you visit.

Save your options before exiting.

X-10. NoScript:

Block dangerous scripting, while allowing needed exceptions.
See <http://noscript.net/>



NOSCRIPT

Security	++
Privacy	+/-
Simplicity	--
Cost	0
Usability	--
Performance	0

Targeted risk: malicious JavaScript

A caution about NoScript: at first, it may drive you crazy as it asks you what to do about tons of sites. This will settle down over time, if you're like most Internet users.

Note, too, that if you do disable scripting on some or all sites, those sites may not work well (if at all).

On the other hand, if you enable scripting everywhere, you will be exposing yourself to scripting holes large enough to drive a truck through.

NoScript currently flags properly functioning Shibboleth federated login sites as a potential cross site scripting vulnerability.

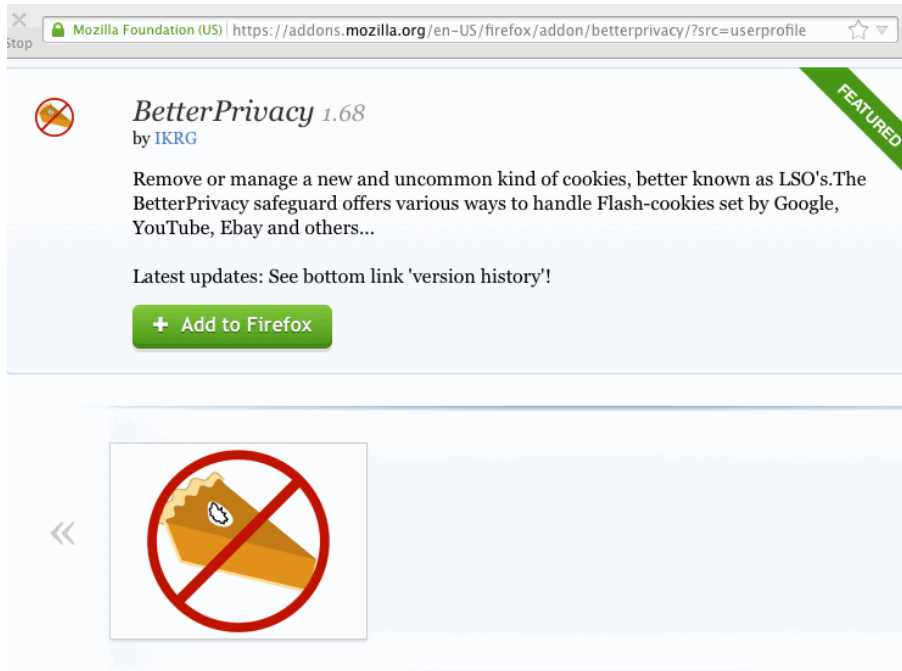
You should also be aware that NoScript "whitelists" some sites by default; see: http://noscript.net/faq#qa1_5 (you may or may not agree with those whitelisting decisions)

Another consideration: maintaining a list of "allowed" scripting sites in NoScript represents a potential privacy exposure if a forensic review of your system is performed.

X-11. *Better Privacy*

In addition to regular cookies, some programs may also attempt to set so-called Flash "Super-cookies."

Better Privacy is a Firefox add-on that will let you block or remove those.

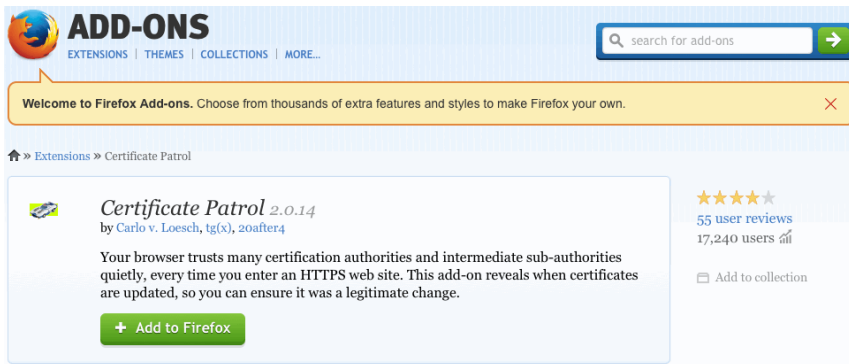


BETTER PRIVACY

Security	++
Privacy	+/-
Simplicity	--
Cost	0
Usability	--
Performance	0

Targeted risk: Flash super cookies

X-12. Certificate Patrol



CERTIFICATE PATROL

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: man-in-the-middle attacks on secure sites

Globally trusted SSL/TLS certificates obtained from commercial certificate authorities are widely used on the Internet for secure web sites (online shopping sites, banks, airlines, etc.), and are key to deterring man-in-the-middle (MIM) attacks.

Unfortunately, it's currently technically possible for any certificate authority to issue a globally trusted certificate for any web site.

Certificate Patrol helps you watch for "unexpected certificate changes," as might be seen if an improperly obtained certificate were to be installed on a host that's then used to conduct a MITM attack. It does this by keeping track of the certs you've seen, letting you know when one changes so you can give that change a close(r) look if that change was premature or otherwise unexpected.

X-13. RefControl

When you click on a link and go to a new web page, the new web site is told where you came from -- maybe you clicked on a link in a search engine, or a link on a web page, for example.

The information about where you came from is normally called a "Referrer" string.

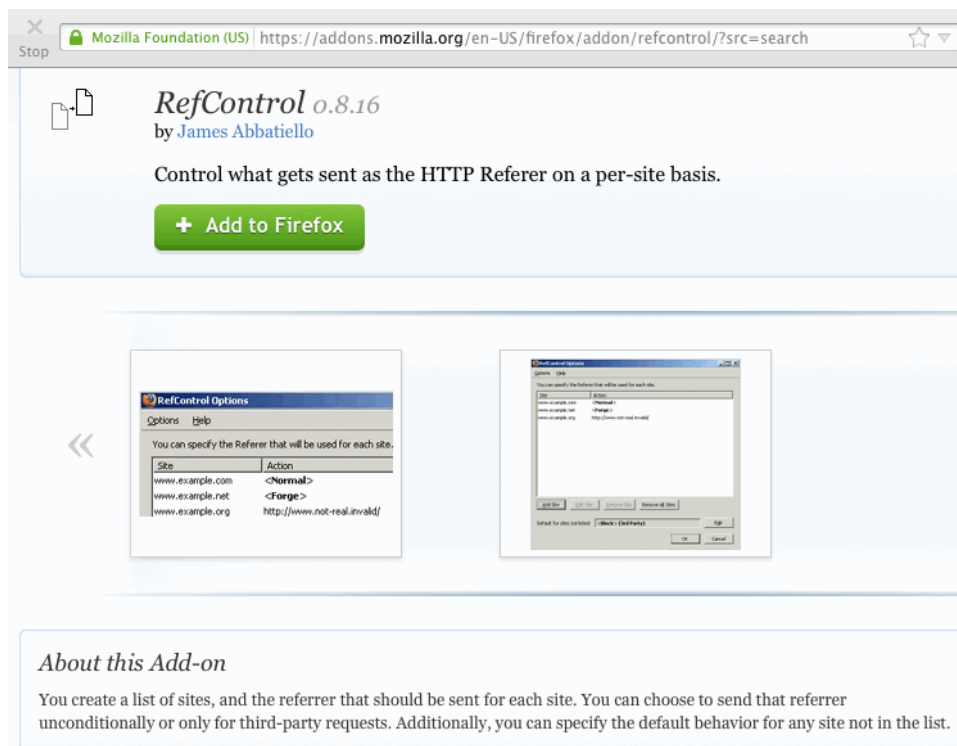
While it can be helpful for a site to know where its visitors are originating, it can (at times) also result in your privacy being compromised. Therefore, you may want to routinely block referrer strings when visiting most web pages.

One easy way to do this is with the RefControl add on, see <http://www.stardrifter.org/refcontrol/>

REFCONTROL

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: Bleedthrough of referrer information



After installing RefControl, go to Add-ons Manager --> RefControl --> Preferences and set the "Default for sites not listed: Block"

Note: Some sites may refuse to let you access some of their content unless a valid referrer is provided.

X-14. Changing the user agent string.

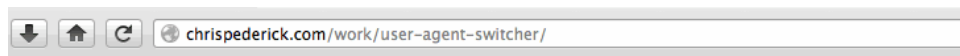
Like the referrer string, the user agent string is sent by your browser when a web page gets requested. It identifies your computer's operating system and browser, down to and including version details. This information allows a site to tailor the web content it provides for your system, but... an accurate user agent string can also allow malicious web sites to easily identify vulnerabilities associated with the operating system and/or the web browser you're using.

Providing an inaccurate/intentionally misleading user agent string can make it harder for the bad guys to target your system. For example, you might change your user agent string so that your system pretends to be Internet Explorer 10 on a Windows 8.1 system rather than accurately self-reporting that it is a Mac OS X Mavericks laptop running Firefox 27.0.1. An attacker seeing that user agent string might then try IE or Windows 8.1 exploits rather than Mac OS X or Firefox exploits. You can even try pretending to be a smart phone or a search engine web crawler.

Unfortunately, changing your user agent string also regrettably increases the likelihood that the web sites you visit won't work quite right. For example, if you change your user agent string to make it look like you're actually a smart phone, you might end up with the mobile version of a web site, set up to display right on a small screen.

If, notwithstanding this risk of getting screwed-up legitimate pages, you'd still like to try this defensive approach, User Agent Switcher is a Firefox add-on that will allow you to easily change your browser's user agent string:

USER AGENT SWITCHER	
Security	+
Privacy	+
Simplicity	--
Cost	0
Usability	--
Performance	0
Targeted risk: tailored malicious content	



USER AGENT SWITCHER

[DOWNLOAD](#)
[FEATURES](#)
[HELP](#)
[SCREENCASTS](#)
[FORUMS](#)
[SOURCE](#)

The User Agent Switcher extension adds a menu and a toolbar button to switch the user agent of a browser. The extension is available for [Firefox](#) and will run on any platform that this browser supports including Windows, OS X and Linux.

A sample report from <http://whatsmyuseragent.com/> after changing the user agent to pretend to be an iPhone:

The screenshot shows a web browser window with the address bar displaying 'whatsmyuseragent.com'. The page title is 'What's My User Agent?'. The main content area displays the user agent string: 'Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16' and the IP address: '98.232.224.128'. A sidebar on the right, titled 'The Elements of Your User Agent String Are:', lists the components of the string: Mozilla/5.0, iPhone, U, CPU iPhone OS 3_0 like Mac OS X, en-us, AppleWebKit/528.18, KHTML, like Gecko, Version/4.0 Mobile/7A341, and Safari/528.16. Below the main content, a section titled 'Recent User Agents Visiting this Page:' lists two recent user agents, with the first one being the same as the current user's.

What's My User Agent?

Your User Agent String is:

Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Your IP Address: **98.232.224.128**

"What's My User Agent?" allows you to view details about your user agent, along with other information your browser sends to this website.

Recent User Agents Visiting this Page:

1. **You!! Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16**
2. Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en)

The Elements of Your User Agent String Are:

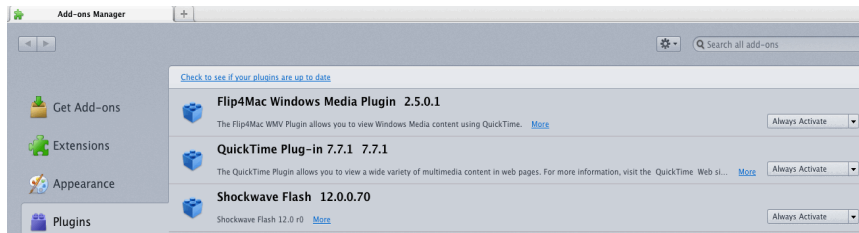
- Mozilla/5.0
- iPhone
- U
- CPU iPhone OS 3_0 like Mac OS X
- en-us
- AppleWebKit/528.18
- KHTML
- like Gecko
- Version/4.0 Mobile/7A341
- Safari/528.16

X-15. Patching Plugins, Browser Extensions and Helper Apps

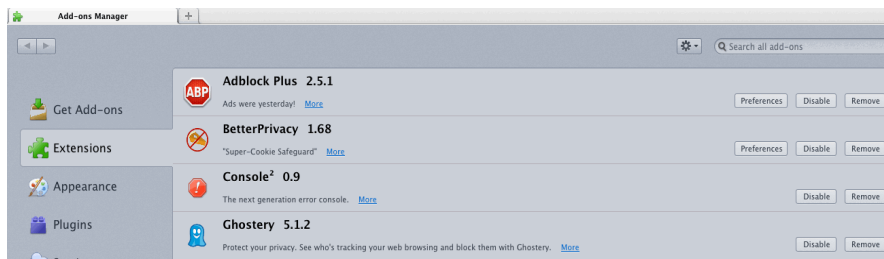
Many browser security issues are associated with insecure/unpatched plugins or browser extensions. It is critical that you keep those up-to-date.

Begin by disabling or completely uninstalling any plugins or extensions that you don't routinely use.

-- Check what's installed at Firefox --> Tools --> AddOns --> Plugins. Disable any plugins you know you don't need or use.



-- Next check what's installed at Firefox --> Tools --> AddOns --> Extensions. Again, disable any installed extensions you don't need or use.



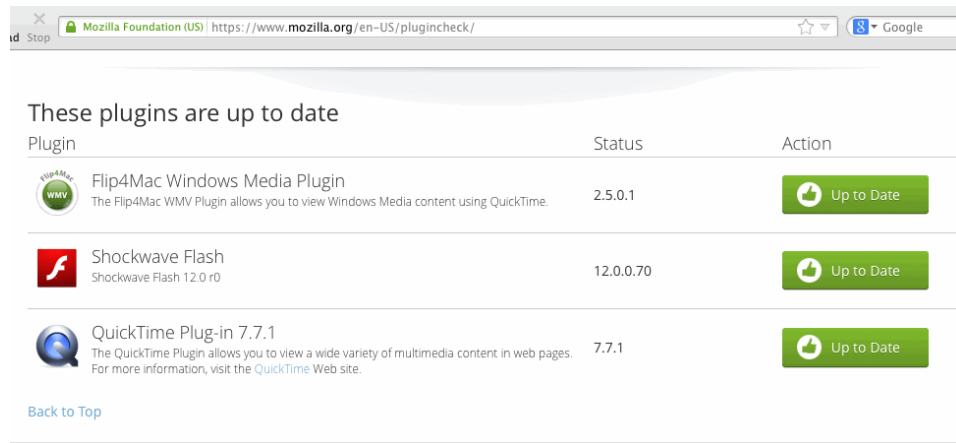
PATCHING PLUGINS

Security	++
Privacy	+/-
Simplicity	--
Cost	0
Usability	--
Performance	0

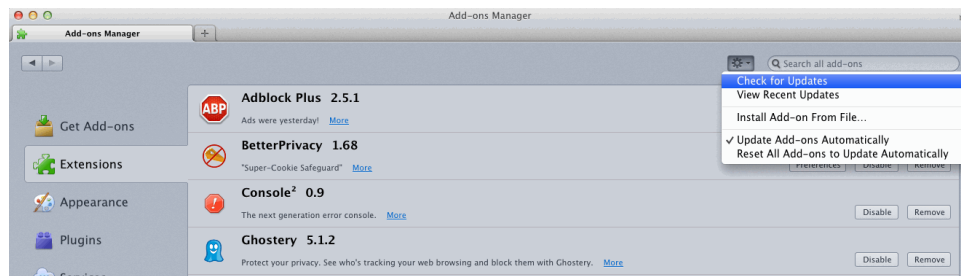
Targeted risk: malicious JavaScript

Now run Firefox PluginCheck.

The easiest way to do this is by going to: Firefox --> Tools --> AddOns --> Plugins --> "Check to see if your plugins are up-to-date." That link will open PluginCheck:



Next, check for updates to browser extensions by going to Firefox --> Tools --> AddOns --> Extensions --> Gear Menu --> Check for Updates.

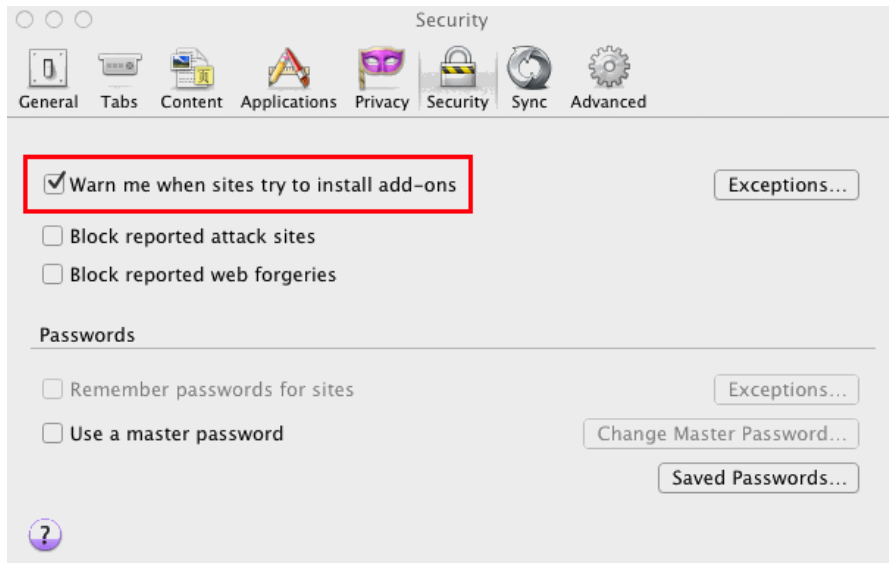


Also check to be sure that Firefox --> Tools --> AddOns --> Extensions --> Gear Menu --> Install Updates Automatically is also selected.

X-16. Configuring the Browser for Better Security

X-17. Warn me when sites try to install add-ons

Firefox --> Preferences --> Security



Ensure that there are also no "Exceptions" listed (see the "Exceptions..." button shown above)

X-18. Block reported attack sites; block web forgery sites.

Tick the boxes in the same panel shown above.

Read the Firefox privacy policy for a discussion of how this service works.

WARN NEW PLUGINS

Security	++
Privacy	0
Simplicity	0
Cost	0
Usability	0
Performance	0

**Targeted risk: surreptitious
malicious plugin addition**

BLOCK BAD SITES

Security	++
Privacy	-
Simplicity	0
Cost	0
Usability	0
Performance	0

**Targeted risk: malicious
web sites**

X-19. Do NOT use "remember passwords for sites"

The "Remember passwords for sites" box should be **UNCHECKED**, as shown above.

If you examine the "Saved Passwords..." button, no saved passwords should be listed.

If you need to save passwords, consider using a separate and cryptographically secure password manager, as previously discussed.

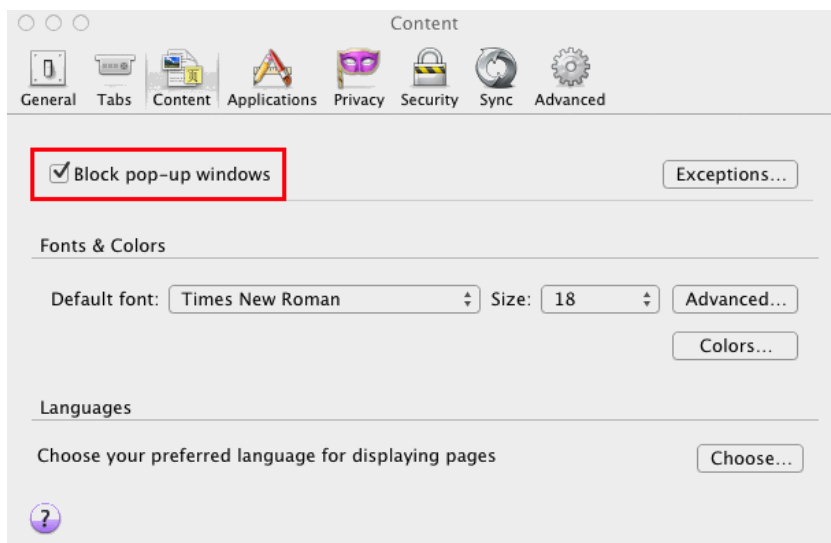
DON'T SAVE PASSWORDS

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: password harvesting

X-20. Block pop-up windows

Firefox --> Preferences --> Content



BLOCK POPUPS

Security	+
Privacy	0
Simplicity	+/-
Cost	0
Usability	+/-
Performance	0

Targeted risk: popunders; aggressive advertising

X-21. Choose helper applications for file types

Firefox --> Preferences --> Applications

This preference pane determines how Firefox handles different types of files, such as .pdf files. Do you want to open them with a particular application? Just save the file to disk? "Always Ask," allowing you to decide on a case-by-case basis?

In some cases you may have multiple applications installed that can handle a given file type. The default choice will often be fine, but advanced users may wish to substitute an alternative application for the default in some cases.

See also the discussion at

<https://support.mozilla.org/en-US/kb/set-how-firefox-handles-different-file-types>

HELPER APP CHOICE

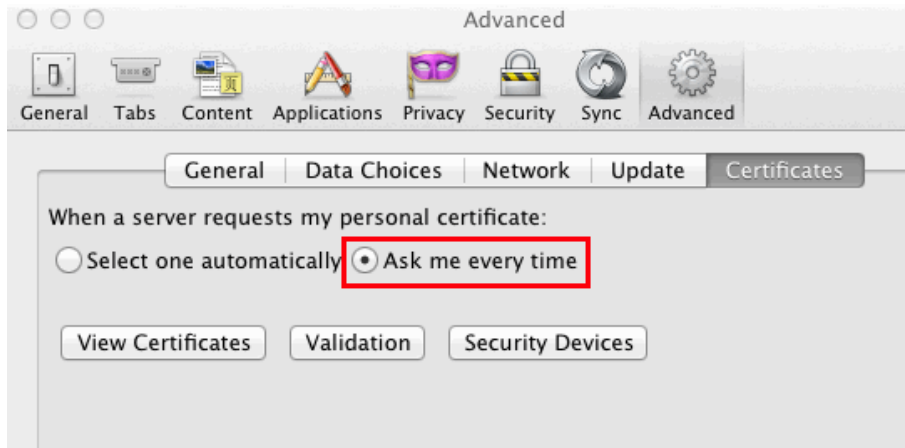
Security	+
Privacy	0
Simplicity	-
Cost	0
Usability	+/-
Performance	0

Targeted risk: exploitable default helper applications

X-22. Personal Certificate Privacy

Firefox --> Preferences --> Advanced --> Certificates

Select "when a server requires my personal certificate, ask me every time"



CERTIFICATE HANDLING

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: exploit PKI to identify users visiting a site

General recommendation: store any personal certificates you may use in a USB-format PKI hard token or smartcard, not in-browser, and only insert and "unlock" that hard token or smartcard when you need to use your cert.

X-23. Recommended Browser Preference Settings for Improved Privacy.

X-24. Set a blank home page or use a privacy-preserving search engine as your start page.

Many users routinely set Google (or perhaps Bing) to be their default home page. This potentially tells Google (or other search engine providers) a lot about when/where you use the web.

A more private choice is to either set your home page to be blank, or to set it to use a privacy-preserving search engine, instead.

Firefox --> Preferences --> General

Either: "When Firefox starts: Show a blank page"

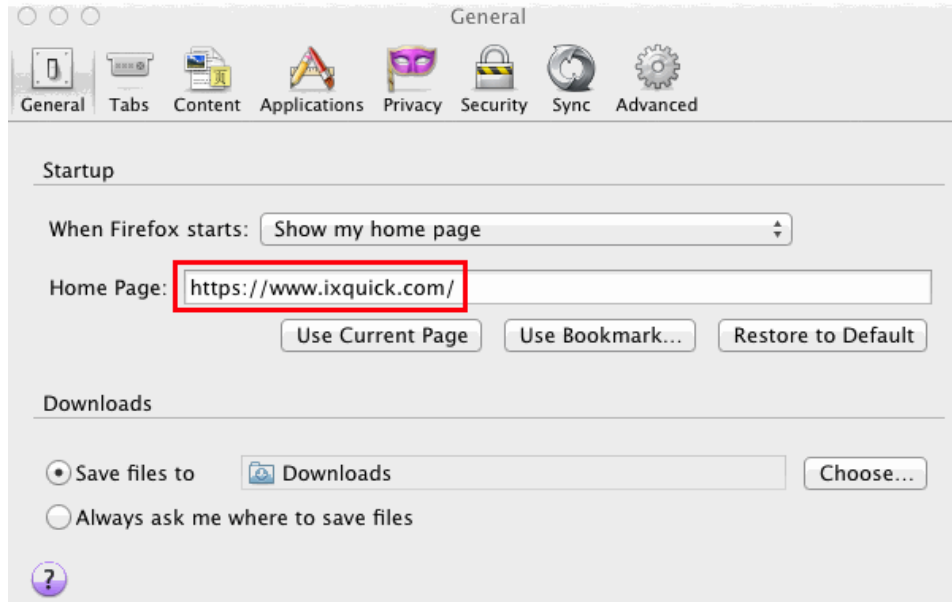
Or:

"When Firefox starts: Show my home page" with your home page set to one of the following alternative search engines:

-- <https://duckduckgo.com/>

-- <https://www.ixquick.com/>

For example:



HOME PAGE CHOICES

Security	0
Privacy	++
Simplicity	0
Cost	0
Usability	0
Performance	0

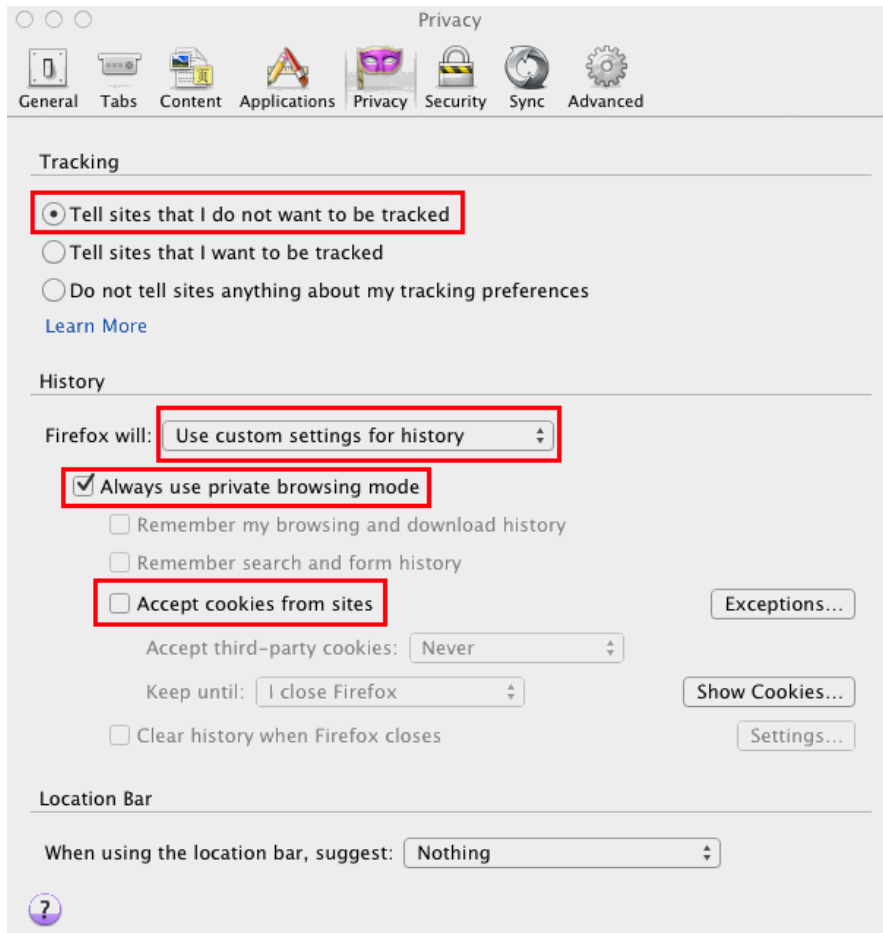
Targeted risk: tracking by search engine providers

If, notwithstanding the above, you do decide to continue to use Google as your default search engine, avoid being logged in to your Gmail account while using Search. If you have already done so in the past, you may want to clear your search history.¹¹⁹

¹¹⁹ <https://support.google.com/websearch/answer/465?hl=en>

X-25. Tell sites that I do not want to be tracked, always use private browsing mode, and reject cookies

Firefox --> Preferences --> Privacy



COOKIES, ETC.

Security	0
Privacy	+++
Simplicity	-
Cost	0
Usability	-
Performance	0

Targeted risk: tracking by web sites; local forensics

While you're on that panel:

- Set the browser to "Use custom settings for history"
- Always use private browsing mode
- UNCHECK "Accept cookies from sites." (note: some sites may not work w/o at least session cookies)

X-26. Disable local cached web content

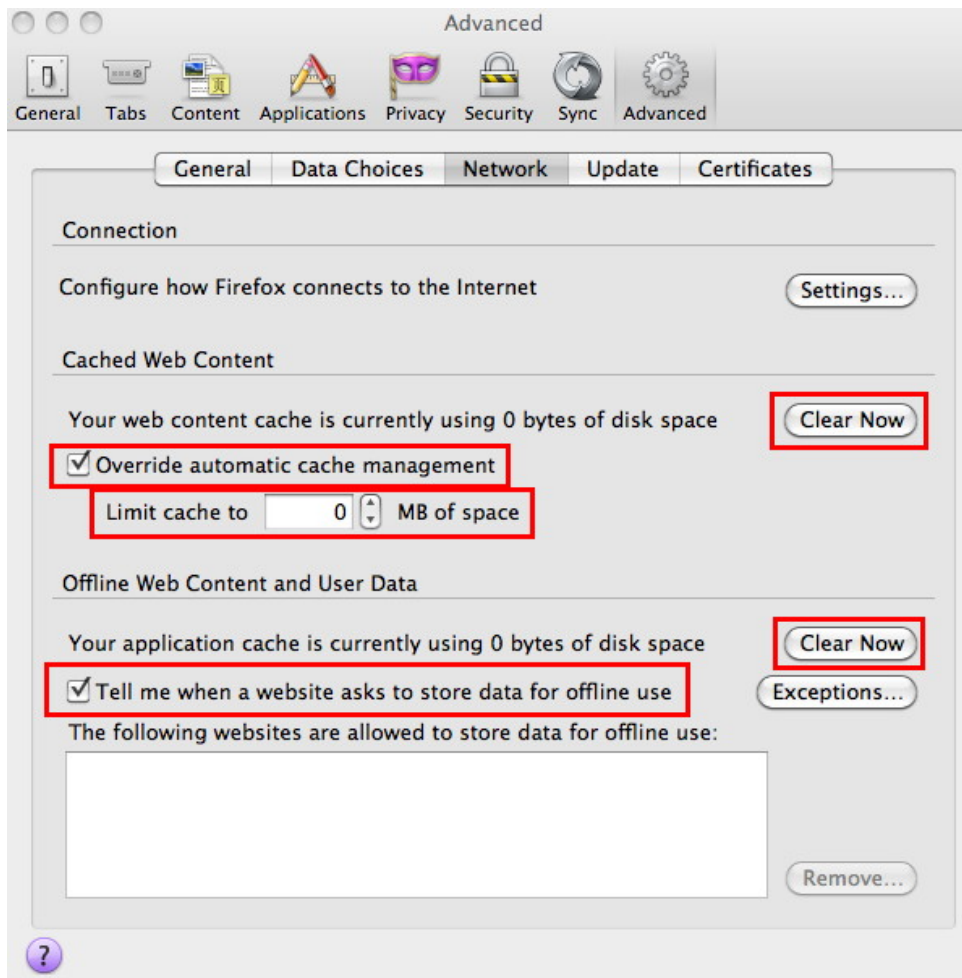
Firefox --> Preferences --> Advanced --> Network

- Clear web cache now by clicking on the "clear now" button
- Override automatic cache management: checked
- Limit cache to 0 MB
- Clear application cache now by clicking on the "clear now" button
- Tell me when a website asks to store data for offline use: checked
- Ensure no exceptions are listed in the "Exceptions" button

LOCAL WEB CACHING

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	-

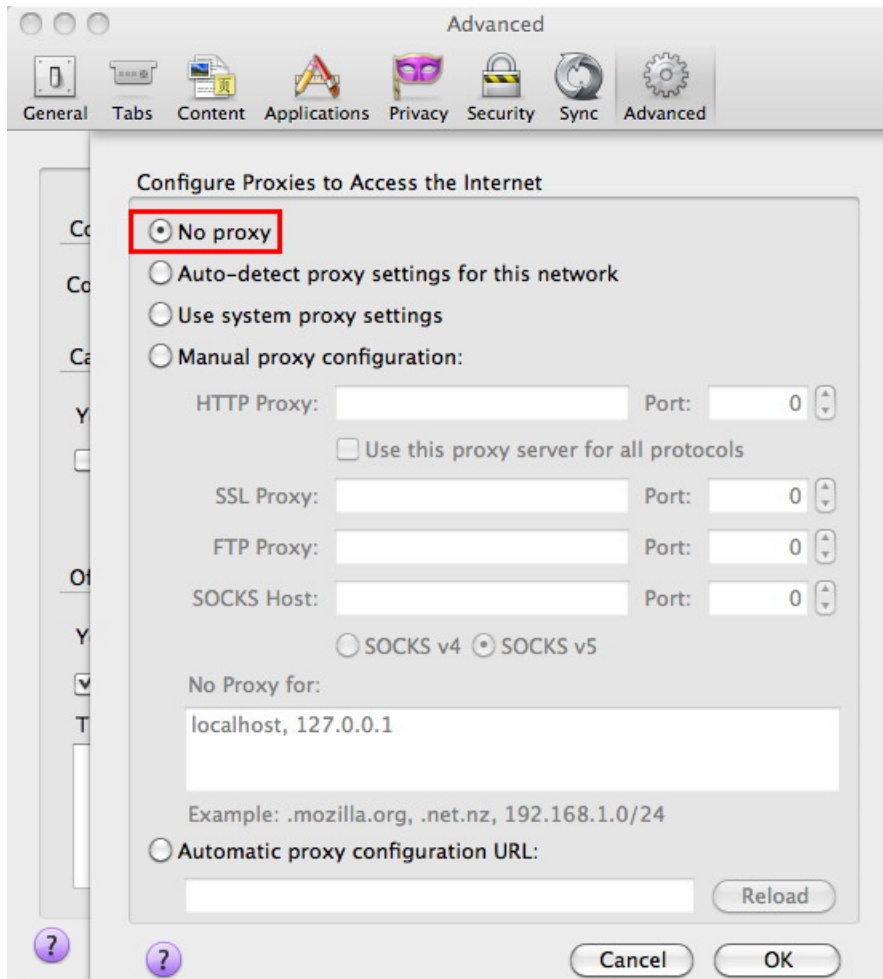
Targeted risk: local forensic review



X-27. Connect directly, not via a proxy server

Some sites send all local web traffic through a "web cache" or "proxy server." We've previously discussed this at the operating system level; we now consider this issue from the perspective of the web browser, ensuring that your Firefox is ALSO configured to NOT use a local proxy server.

Firefox --> Preferences --> Advanced --> Network --> Settings



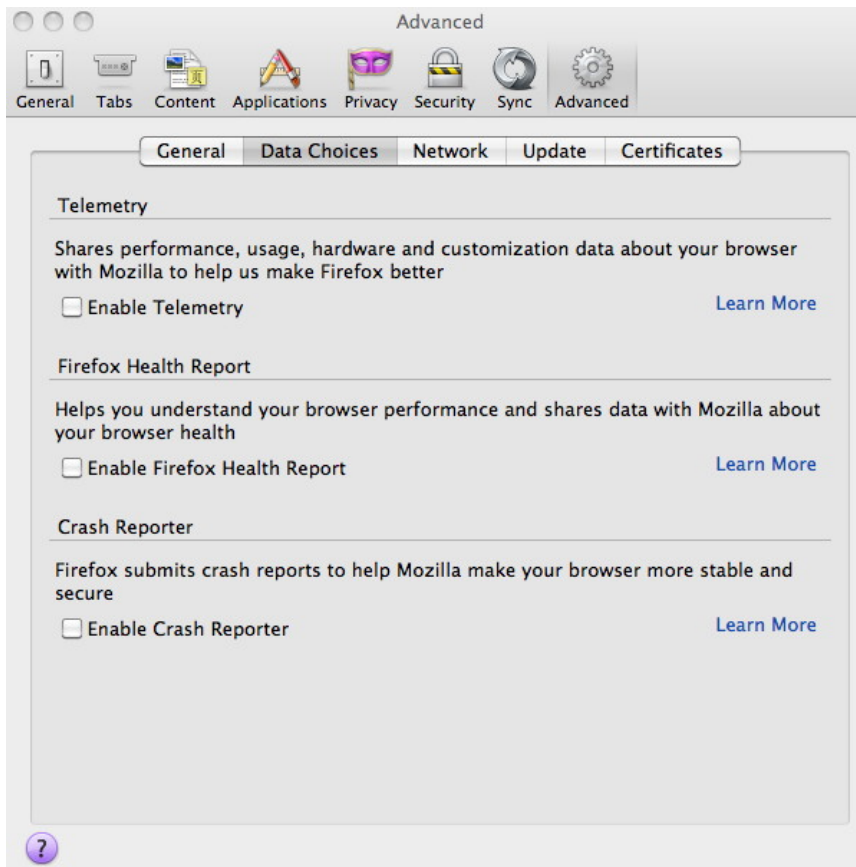
BROWSER AND PROXIES

Security	-
Privacy	++
Simplicity	+
Cost	0
Usability	+
Performance	-

Targeted risk: potential local content monitoring

X-28. Do not enable telemetry, health reports or crash reports

Firefox --> Preferences --> Advanced --> Data Choices

**DATA CHOICES**

Security	-
Privacy	+
Simplicity	0
Cost	0
Usability	0
Performance	0

**Targeted risk: usage info
bleed to browser vendor**

X-29. Device synchronization features

Firefox --> Preferences --> Sync

If you use Firefox on multiple devices, you might be tempted to keep "state" synchronized across all those devices so that you have the same bookmarks, for example, everywhere.

While synchronized data is encrypted before transmission, we would still urge privacy-conscious users to avoid sync'ing.

DEVICE SYNC

Security	0
Privacy	+
Simplicity	-
Cost	0
Usability	-
Performance	0

**Targeted risk: increased
privacy exposure (n devices)**

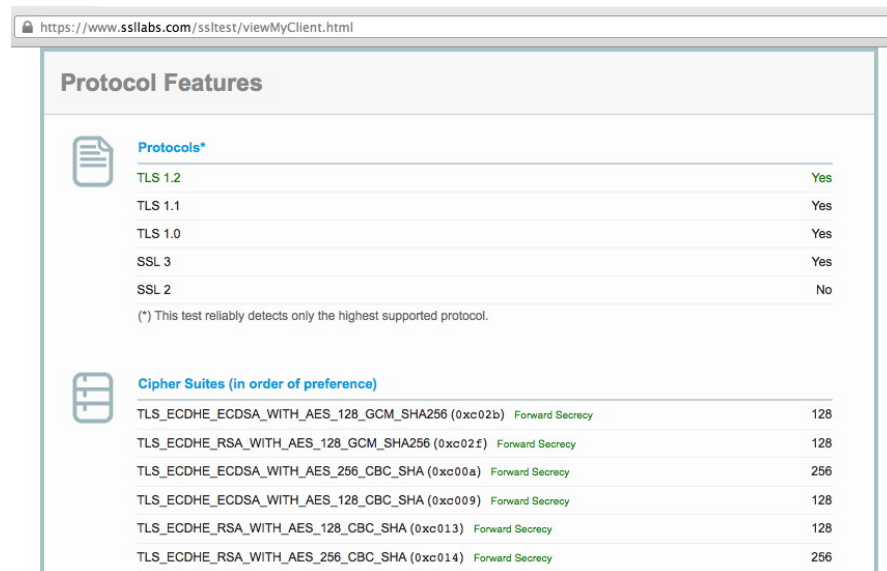
X-30. Secure Web Sites and SSL/TLS Support in Firefox

Firefox supports secure connections to sites that use SSL/TLS (e.g., URLs that begin "https")

X-31. Firefox Support for TLS 1.2 and Strong Ciphers with Forward Secrecy

You can confirm that your browser is doing SSL/TLS the way it should by visiting:

<https://www.ssllabs.com/ssltest/viewMyClient.html>



The screenshot shows the 'Protocol Features' section of the SSL Labs test results. It lists supported protocols and cipher suites with their respective security levels and forward secrecy support.

Protocol Features		
Protocols*		
TLS 1.2		Yes
TLS 1.1		Yes
TLS 1.0		Yes
SSL 3		Yes
SSL 2		No
(*) This test reliably detects only the highest supported protocol.		
Cipher Suites (in order of preference)		
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	Forward Secrecy	256

TLS 1.2 + FWD SECRECY

Security	+
Privacy	+
Simplicity	-
Cost	0
Usability	0
Performance	0

**Targeted risk: obsolete TLS;
retrospective decryption**

You should be seeing TLS 1.2 supported ("Yes") and you should see cipher suites listed as supporting forward secrecy.

You can also test your browser's cipher support with <https://cc.dcsec.uni-hannover.de/>

X-32. Ensure that OCSP/CRL Is Used (and Required, If Possible)

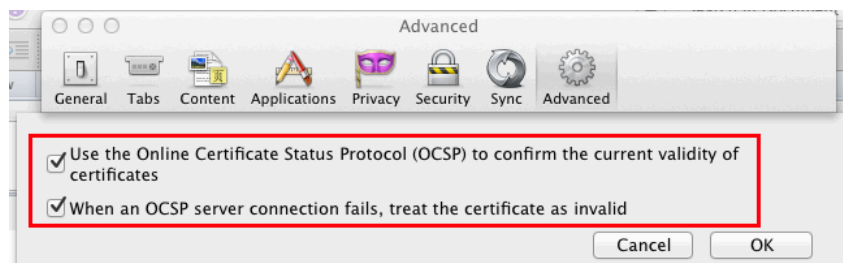
When Firefox visits a secure web site, it checks to see if the cert that sites present is valid, including checking to see if the cert has been revoked. Firefox normally does this with OCSP, the Online Certificate Status Protocol. Some browsers don't bother to check, or if they don't get a response, assume that everything's okay.

The security conscious choice is to require OCSP checks, and to assume the worst if no response is received from the OCSP server.

To check the settings on your browser, go to:

Firefox --> Preferences --> Advanced --> Certificates --> Validation

Ensure that you're set to use OCSP and that you're also set to treat OCSP connection failures as invalid certificates:



Caution: OCSP server failures can block access to some secure sites when set up this way, e.g., if there's a problem accessing the OCSP server.

Caution: Requiring OCSP checks can interfere with use of some captive portal sites (you need to trust the SSL/TLS-secured site to be able to connect, but you can't connect until you can verify the OCSP status of the associated certificate, a circular dependency that may result in a deadlock). See <https://wiki.mozilla.org/CA:OCSP-HardFail> for more information.

Caution: OCSP checks potentially bleed information about the sites you're visiting to a third party (e.g., the CA operating the OCSP responder)

X-33. Trust anchors

The SSL/TLS certificates that Firefox trusts by default can be seen here:

<http://www.mozilla.org/en-US/about/governance/policies/security-group/certs/included/>

You may also be interested in the status of pending request for inclusion that are listed here:

<https://wiki.mozilla.org/CA:Schedule>

Technical users may want to confirm that they're only trusting the trust anchors that are associated with companies or governments that they personally are comfortable trusting.

REQUIRE OCSP

Security	+
Privacy	-
Simplicity	-
Cost	0
Usability	-
Performance	-

**Targeted risk: revoked
certs in use by 3rd parties**

X-34. Firefox making connections w/o me doing anything????

Normally, you might expect that if you were using your computer, it wouldn't be doing anything.

However, if you run LittleSnitch or some other product that focuses on monitoring outbound connections, you may notice that Firefox sometimes makes outbound connections even if you aren't doing anything.

<https://support.mozilla.org/en-US/kb/how-stop-firefox-automatically-making-connections> discusses a variety of reasons why this might be happening, and explains the steps you can take to make it stop.

X-35. Protecting the User's Privacy: Browser Fingerprinting

If you login to a web site, accept persistent cookies, or consistently use the same static IP address, you should not be surprised if you are uniquely trackable. You may be surprised, however, to find out that you may be uniquely trackable simply based on the "fingerprint" of your browser.

The Electronic Freedom Foundation has a browser fingerprint tester that you can try if you'd like to see:

<https://panopticklick.eff.org/>

Do not be surprised if you find that your browser is quite easily fingerprinted based just on factors such as your "User Agent" string, browser plugin details, system fonts, etc.

If you are distressed by what you see, ensure that you have Javascript disabled (either entirely, or with NoScript). If you were accidentally allowing Javascript to run on that site, disable it and then visit the site again -- you will likely notice a substantial improvement in the reported fingerprintable characteristics.

Another testing site you can try: <http://ip-check.info/?lang=en>

Digging in further: <http://browserspy.dk/> does a nice job of offering service-by-service tests for a broad range of potentially fingerprintable characteristics.

<https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability> provides a detailed technical discussion of factors that may contribute to your browser session being readily trackable even if you aren't logged in and haven't been accepting cookies.

See also <https://wiki.mozilla.org/Fingerprinting>

You can reduce the fingerprints you leave behind, but note that by doing so you may need to take steps that make some sites subtly malfunction or cease to work entirely.

XI-1. Deep Settings: Firefox and about:config settings.

Some Firefox settings ("deep settings" or "advanced settings") can only be accessed via the Firefox "about:config" mechanism. Firefox doesn't expect most users will -- or should -- change these settings. If you decide to do so, we emphasize that you do so at your own risk.

A (LONG!) list of about:config security- and privacy-related preferences can be seen at:
http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences

We'll just consider a few of those settings by way of example.

a) Prefetching

Prefetching attempts to anticipate the content you will likely want or need based on hints in the web page, and attempts to download that content in advance.¹²⁰ If you'd prefer to only download content you explicitly want, disable pre-fetching:

- In the Location bar, type about:config and press Return.
- The about:config "This might void your warranty!" warning page may appear. Click I'll be careful, I promise! to continue to the about:config page.
- Hold down the Ctrl key while you click in the list of preferences, select New, and then select Boolean.
- In the Enter the preference name window, enter network.dns.disablePrefetch and click OK.
- Select true when prompted to set the value and click OK.

If you want to disable prefeteching, you should also set network.prefetch-next to be false.

b) Geo-Enabled

Quoting the Firefox documentation, "Firefox can tell websites where you're located so you can find info that's more relevant and more useful."¹²¹ You may want to permanently disable that functionality. To do so:

- In the URL bar, type about:config
- Type geo.enabled
- Double click on the geo.enabled preference (so it is set to be "false")
- Location-Aware Browsing is now disabled

c) DOM-storage

Quoting from <https://developer.mozilla.org/en-US/docs/Web/Guide/API/DOM/Storage> --

DOM Storage is the name given to the set of storage-related features first introduced in the Web Applications 1.0 specification, and now split off into its own W3C Web Storage specification. DOM Storage is designed to provide a larger, more secure, and easier-to-use alternative to storing information in cookies.

Just as we generally don't like content being stored in cookies, we also don't like information stored in DOM storage, either (even if you don't hear as much about DOM storage being used for tracking purposes).

To disable DOM storage, see <http://kb.mozillazine.org/Dom.storage.enabled>

¹²⁰ https://developer.mozilla.org/en-US/docs/Link_prefetching_FAQ

¹²¹ <http://www.mozilla.org/en-US/firefox/geolocation/>