A Guide to Hardening Your Browser

This guide provides experience-based advice based on the things we do to protect our own computers against people like us. Some of it may go against the grain; some may conflict with advice you've received in the past; some things may be missing entirely. However, if you implement the advice presented herein you will stand a good chance of thwarting the majority of modern APT and AVT ("Advanced Persistent Threat" and "Advanced Volatile Threat") attacks against your Mac OS X system.

Background

Conventional wisdom tells us a few things about securing a laptop against viruses, trojans, et al:

- Apply security patches.
- Use anti-virus.
- Don't open untrusted attachments.
- Don't download shady programs from the Internet (eg. keygens or software cracks).

Sometimes conventional wisdom lets us down. Recently some big names have been in the headlines: Apple, Facebook, Microsoft. They all got owned, and they got owned in similar ways:

- Specially-crafted malware was targeted at employee computers, not servers.
- The malware was injected via a browser, most often using malicious Java applets.
- The Java applets exploited previously unknown "0day" vulnerabilities in the Java VM.
- The Internet browser was the vector of choice in all cases.

What does this tell us?

- Patching doesn't help: It goes without saying that there are no security patches for 0day.
- Anti-virus won't work: It was custom malware. There are no AV signatures.
- No attachments to open: Attacks are triggered by simply visiting a web page.
- No shady websites required: Attacks are launched from trusted advertising networks embedded within the websites you visit.
- We need to lock down our browsers.

Assumptions

- You are the target of a highly-skilled, well-funded attack team (e.g. a nation state).
- They have access to multiple 0day exploits that affect your Internet browser.
- They have the means to "infect" the websites you visit every day (e.g. stackexchange.com) by loading 0day into your browser via 3rd party websites (e.g. advertising, metrics, or SEO networks).
- You have a MacBook or other OS X-based computer.

If you are the target of an attack in this scenario you will probably get owned sooner rather than later unless you take extra precautions. Given that the browser is currently the weakest link in your security chain, we will tackle it head-on and revise the way in which we think about securing our day-to-day Internet browsing.

Handling the Issue

The process of defending against sophisticated browser zero-day attacks will be broken down into three sections:

1. Reduce the attack surface:
   - Disable problematic browser plugins
   - Block advertising hosts/domains
   - Install defensive extensions
   - Change your browser User Agent
   - Encrypt your DNS queries
2. Limit the scope for damage in the event of compromise:
   - Sandbox your browser
   - Sandbox your other common internet apps (IM, mail)

ABOUT STACH & LIU

Founded in 2005, Stach & Liu is a global security consulting firm that helps companies secure their networks and applications. Our services include network and application penetration testing, application source code review, network risk assessment, security policy and compliance review, and strategic security consulting.

With over 250 years of combined experience, each member of the Stach & Liu team brings distinct expertise and perspective to the table. We put our background in government intelligence, the Fortune 100, Big 4 consulting, and global security to work for our clients.

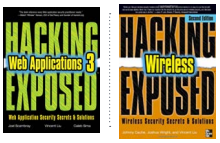
SELECTED CERTIFICATIONS

CISA — Certified Informtion Systems Auditor

6Sigma

CISSP — Certified Information Systems Security Professional

SELECTED PUBLICATIONS



CONTACT

Stach & Liu, LLC
4600 E. Washington Street,
Suite 300
Phoenix, AZ 85034
480 621 8967
contact@stachliu.com
www.stachliu.com

facebook.com/stachliu

@stachliu

linkedin.com/company/stach-&-liu

3. Change your browsing habits:
   - Use your hardened browser at all times
   - Never use public wifi without a VPN
   - Never save passwords in your browser
   - Use a password safe

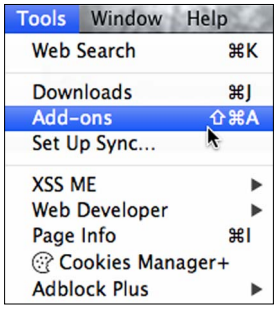
Step 1 – Reduce your Attack Surface

Pick a Browser

This guide assumes you are using Firefox as your browser – your only browser. We will lock this browser down to become your "daily Internet use" browser. The idea is to create a browsing environment that sacrifices some usability in the name of a more hardened attack surface. If you use Chrome, Safari, Opera, or another browser, most of the recommendations will still be relevant; although URLs, screenshots, and walk-throughs will differ somewhat.

Disable Problematic Browser Plugins

There is no reason to enable Java in your browser. It has a very poor security track record and is a major security risk. Disable it immediately by going to Firefox's add-ons:



You should see something like this:

If you see "Java" in that list, click the "Disable" button next to it. You can leave Flash alone for now – we will lock that down later.

Note: If for some reason you need to run Java in your browser then refer to the "Help" section of the "NoScript" browser extension (discussed later). NoScript will help you whitelist the websites that are allowed to use Java, however this is not recommended and should be done only if you require Java in your browser for business purposes.

Block Advertising Networks (Plugin Method – Recommended)

Adblock Plus

https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

This browser plugin blocks requests to advertising networks. It maintains an automatically updated blacklist of advertising hosts and domains and stops Firefox from loading any content located on them.

Pro: By blocking advertising networks, you make it vastly more difficult for attackers to load malicious adverts in your browser. This, in turn, makes it far more difficult to reliably target your browser, which makes it difficult to target you.

Con: Adblock is great. Please consider donating. It should be noted, however, that by installing extensions into your browser you are installing executable code that could be compromised. The likelihood of such an attack is low, but not, as Vizzini would say, inconceivable.

Block Advertising Networks (Hosts File Method – More Complex)

You can download a special hosts file to concatenate to your local /etc/hosts file that will redirect all known advertising servers to 127.0.0.1. See *http://winhelp2002.mvps.org/hosts.htm* for more information and to retrieve a copy of the latest advert-blocking hosts file. It is important to manually keep this file up-to-date, which makes this method of blocking advertising networks less viable in the long term in comparison to the Adblock plugin.

Use Browser Extensions to Enhance Security

The idea behind these extensions is to disable active scripting content unless it has been explicitly allowed by you, the user.

NoScript

https://addons.mozilla.org/en-us/firefox/addon/noscript/

This extension implements a "default deny" policy for JavaScript code, which means that no website is allowed to execute JavaScript without first being added to a whitelist; the whitelist is very simple to control using a context menu in Firefox. This policy can be extended to apply to Java and Flash objects.

Pro: Allows scripting code to run only on websites you have pre-approved, thereby preventing many automated attacks hosted on untrusted webservers.

Con: NoScript is initially annoying because it must be "trained" to know about the websites you visit regularly. Once this is done (one time per website) it is seamless.

Flashblock

https://addons.mozilla.org/en-US/firefox/addon/flashblock/

Flashblock replaces all Adobe Flash objects with a placeholder icon. If you want to run the Flash object, simply click the placeholder.

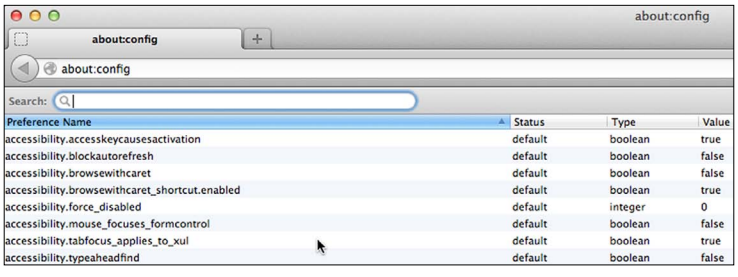
Pro: Prevents Flash apps running automatically, which helps protect against malicious hidden Flash apps embedded in web pages and advertising networks. Sites that you trust (e.g. youtube.com) can be

added to a "trusted sites" whitelist.
Con: Flash apps (except those on your whitelist) will never run automatically, which could negatively affect the usability of a small number of websites.

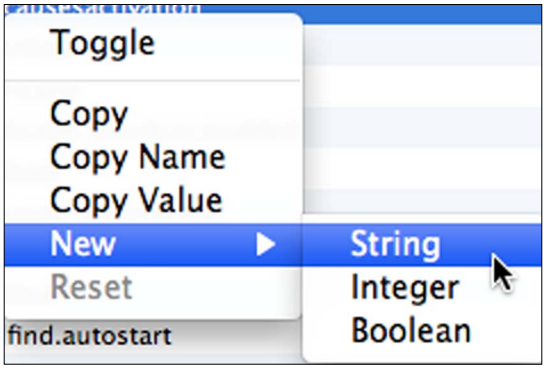
Ghostery
http://www.ghostery.com/
Ghostery prevents advertising networks from dropping web bugs, cookies, Flash cookies, HTML5 persisted data, and other junk into your browser.
Pro: It becomes very difficult to track you (i.e. your browser) across the Internet. This makes it harder for adversaries to identify you. It also increases your personal privacy.
Con: None. Ghostery is great. Please consider donating.

HTTPS Everywhere
https://www.eff.org/https-everywhere
This extension forces your browser to use SSL/TLS for all communications with the biggest sites on the Internet. For example, http://www.ebay.com will automatically be converted to https://www.ebay.com by this plugin. There are hundreds of websites supported by default, with more being added all the time.
Pro: Forces your browser to use SSL encryption whenever it's supported by a website. This mitigates many attacks, especially man-in-the-middle hijacking. It also makes it easier to detect when an adversary is eavesdropping on your private communications. Note that it doesn't prevent eavesdropping; it simply makes it more difficult to do so without alerting you, the end-user.
Con: None. HTTPS Everywhere is great.

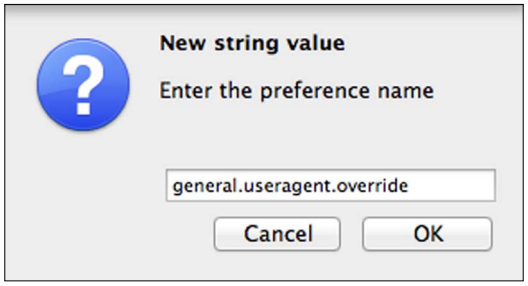
Masquerade as Something Else
Malware often runs in stages where the first is to detect the browser and operating system on which it is running in order to deploy the correct payload. If the malware incorrectly detects your browser or OS it can fail to run, which is good for you. To this end, we reconfigure Firefox to tell sweet, sweet lies. Type "`about:config`" in the address bar:



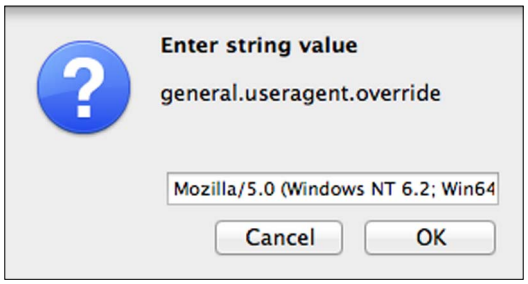
You need to add a new configuration option by right-clicking and choosing New/String.



Call the new string "`general.useragent.override`":



Insert the value "`Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:16.0.1) Gecko/20121011 Firefox/19.0`":



Restart your browser. It will now report itself as Firefox v19 running on Windows 7. Most attempts by malware to detect your browser (and by extension, your OS) will return an incorrect result, which means that an attacker is less likely to deploy the correct exploit to your computer. If you are using a non-Firefox browser such as Chrome, make sure to leave correct browser (e.g. Chrome) information in the User-Agent but change the OS to Windows or Linux; this will allow you to fool malware while still allowing websites to accommodate for browser-specific quirks. Copies of user agent strings are readily available via Google. Please be aware that this method is far from fool-proof and should be viewed as "security by obscurity."

Note: Changing your user agent can lead to annoying side-effects, such as causing websites to incorrectly offer you Windows downloads for your Mac computer.

Step 2 – Limit the Scope for Damage

Let's assume that despite your best efforts at reducing the attack surface, an attacker is able to get 0day running in your browser. At this point AV has failed, patching has failed, plugins have failed, and you just got owned. There are now 2 key factors in play: detection and limiting damage.

It is reasonable to assume that you will not detect the compromise, at least immediately. All your defensive mechanisms have, so far, been thwarted and you are now running attacker-supplied shellcode in your browser. Let's consider what this actually means: an attacker can do anything in your browser that you could do. Further, the attacker can easily spawn new processes, effectively taking control of your computer.

To mitigate the damage that can be done by an attacker in this situation we have to limit the damage that we ourselves could do in this situation. This is because the attacker effectively inherits our permissions; in a successful attack the attacker becomes you. To stop an attacker from doing bad things, you yourself must also be prevented from doing the same bad things. This is the art of compromising usability to provide security. Ask yourself the question: which of my permissions would I like to share with an attacker?

The answer is probably "not many".

The avoidance of getting owned is therefore the art of giving up sufficient daily functionality, so when (not if) an attacker compromises your browser, there is not much they can do with it. To this end we leverage the OS X sandbox.

Sandbox Your Browser

Mac OS X has a relatively unknown and unused built-in application sandbox feature that can be used to lock an application down and control precisely what it is, and is not, allowed to do. For example, the OS X sandbox can be used to:

- Limit which, if any, files can be read, written, or deleted by an application.
- Limit which, if any, external programs canbe launched by an application.

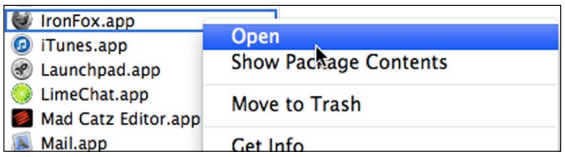
These features are the key to locking down your browser. By restricting the files that Firefox can access, and by preventing Firefox from running new programs, it is possible to restrict the damage an attacker can do. In other words, sandboxing your browser will break much of the custom malware deployed today.

IronFox

https://www.romab.com/ironfox/

The package is a pre-configured OS X sandbox environment for Firefox.

After installing IronFox, you may need to right-click and select "Open" to get around the GateKeeper restrictions (more on these restrictions later).



The main highlights of the sandbox are:

- Necessary files in "/Library" are allowed to be read, not written.
- Necessary files in "/Library" are allowed to be read, not written unless required.
- "/Downloads" is readable and writeable.
- Flash and Java are blocked by default.
- External programs are not allowed to run.

If you need Flash, and you are using the Flashblock plugin, you can tweak the sandbox configuration to enable Flash by editing the file at "/Applications/IronFox.app/Contents/Resources/IronFox.config" and changing the line:

```
FLASH=off     #Enable flash for movies, games, etc
```

To:

```
FLASH=on      #Enable flash for movies, games, etc
```

This can also be done for Java, but it is recommended that Java remain completely disabled at this time. Once installed, you simply run IronFox instead of Firefox. That's it. However, there are some caveats. For example:

- If you download a PDF/dmg/docx/xlsx/etc you will not be able to open it from Firefox unless you reconfigure the sandbox.
- Word documents will not (cannot) open automatically after downloading, nor can you mount disk images (.dmg files) directly from Firefox. If you try you will see an error like this:

The reason for this is that the sandbox prevents Firefox from launching other programs such as Microsoft Word or the diskutil program.

There are a few possible workarounds:

- Configure the sandbox to allow Word, Excel, Preview, diskutil, etc. to be launched by Firefox.
- Use Finder to locate your downloaded file; double-click the file.
- Manually open the correct application (e.g. Word) and manually open the file.

Warning: Sandboxing Breaks Security Updates

There is a very large caveat with using the sandbox: your browser no longer has permissions to install security updates on top of itself. This means that when IronFox prompts you to install security updates, you must follow these steps:

- Close IronFox.
- Open Firefox (running Firefox on its own will always run outside the sandbox).
- From the Firefox menu, choose "About Firefox."
- Click the "Check for Updates" button and follow the instructions.

Sandbox Your Other Internet Applications

The same people who created IronFox also created profiles for the following applications:

- Thunderbird (email client)
- Adium (instant messaging client)
- Safari (Apple's Internet browser)

These three sandbox profiles are beta quality, however if you use any of these apps on a regular basis it is well worth investing the time in setting up a sandbox for them. It is quite literally your last line of defense.

Change your Browsing Habits

Use Your Hardened Browser At All Times

Your browser is hardened for a reason. If you surf the Internet in an unsecured browser (e.g. Safari, Chrome, Opera in this example) you will not be protected and are more likely to get owned. It may be somewhat inconvenient at times to use your hardened browser, but it is far safer.

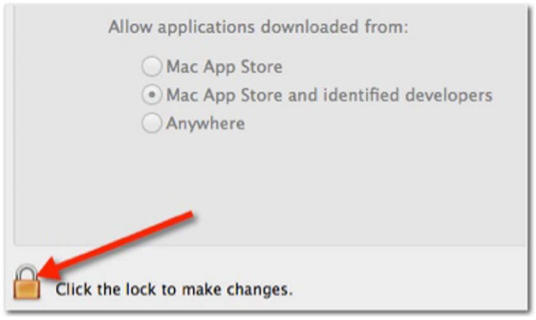
Lock down Anti-Malware and GateKeeper

OS X comes with built-in anti-malware protection. In Lion and later versions, OS X also has the GateKeeper feature.

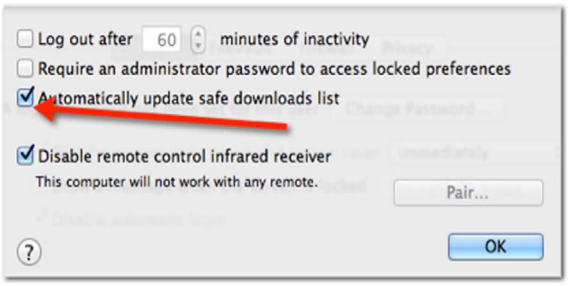
Anti-Malware

This feature scans all of the files you download from the internet and compares them to a blacklist of known malware. The malware list is automatically updated every day. Make sure that automatic updates are enabled by going to System Preferences/Security and Privacy.

Unlock the panel:

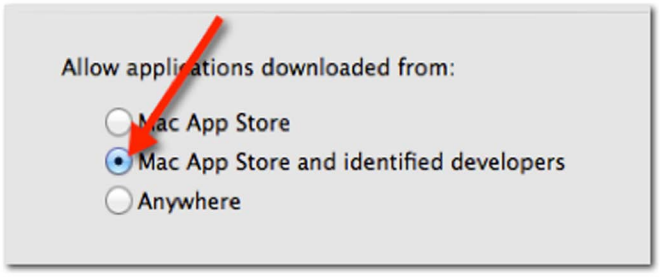


Click the Advanced button and make sure that "Automatically update safe downloads list" is checked:



GateKeeper

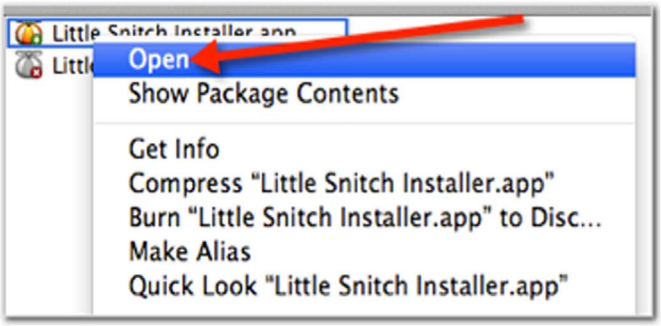
The Security and Privacy settings dialogue gives you more control over the programs that are allowed to run on your computer: The default setting for pre-Lion OS X is "Anywhere", which means any program downloaded from anywhere and written by anyone will be marked as executable. The default for Lion is "Mac App Store and identified developers". By selecting "Mac App Store and identified developers" you restrict the types of files that can be executed to those that are digitally signed by Apple or by a registered Apple developer. Selecting "Mac App Store" will allow you to run only apps downloaded from the Mac App store that have been signed by Apple.



An attempt to run a file that isn't signed results in an error:

The recommended setting is "Mac App Store and identified developers". You will occasionally see an error message if you try to install software that wasn't signed by a registered Apple developer; even double-clicking the file in Finder will not work.

To bypass GateKeeper on a per-application basis, locate the file in Finder, right-click, and choose "Open":



You will be prompted to confirm that you would like to run the program. If you are absolutely sure, click Open to override GateKeeper:

Don't Use Public Wireless Without A VPN

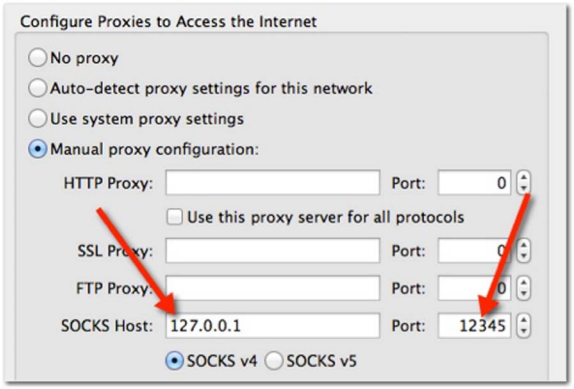
Coffee shop wireless is like playing Russian roulette: one day the bullet will be in the chamber. Someone will hijack your connection, ARP spoof you, Firesheep you, DNS spoof you, man-in-the-middle you, or in some other way ruin your day.

As a consequence, the only safe way to use public services such as GoGo Inflight, Starbucks, airport wifi, etc. is to use some kind of encrypted tunnel.

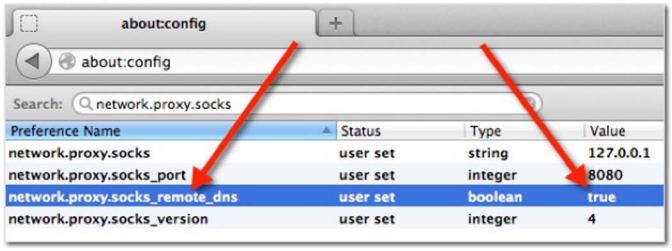
- Work VPN: If you have a work-provided VPN, use it.
- Personal VPN: You can buy cheap VPN service from many providers. One option is a Linode.com server.
- SSH tunnels: The poor man's VPN. If you can SSH into a trusted zone (e.g. work or your own server somewhere) you can use SSH to setup a SOCKS proxy. First SSH into your server, setting up SOCKS as a proxy:

```
ssh -ND 12345 user@host.yourdomain.com
```

After connecting, configure Firefox to use the new SOCKS proxy by going to Preferences/Advanced/Network/Settings. Enter the following information into Firefox's network settings dialog:



Finally, make sure that Firefox DNS queries are done via SOCKS (this is not the default behavior) to prevent DNS spoofing attacks:



Once this is done, the following will occur:

- Your browser will forward all HTTP and DNS traffic over the encrypted SSH tunnel.
- Your connection will appear to come from the remote SSH endpoint.
- All HTTP traffic will be encrypted over SSH, making it infeasible for wireless-based attackers to intercept/modify your traffic.

Encrypt your DNS Queries

DNS spoofing is easy. Just because you type www.google.com into your browser does not necessarily mean that your DNS server will return the correct answer. If an adversary can spoof DNS for you, you will get owned.

To prevent this, it is recommended to use end-to-end encryption for DNS whenever you are not on a trusted network.

DNSCrypt-Proxy

https://www.opendns.com/technology/dnscrypt/

This provides end-to-end encryption of your DNS queries. There is no known way for an attacker to intercept or modify your DNS queries when using DNS encryption. OpenDNS provide this service free of charge.

Don't Save Passwords In Your Browser

If you ask your browser to remember passwords (e.g. using the "remember me" checkbox on many login pages) your password might eventually be stolen. It is better to never use this feature.

Use A Password Safe

Consider storing all of your passwords in a password safe. Protect it using a very, very strong passphrase. This allows you to keep a separate complex password (for example, a Facebook password that is 64 random characters) for every system with which you interact.

The following products are options to consider:

- **1password:** *https://agilebits.com/onepassword*
- **KeePassX:** *https://www.keepassx.org/*
- **LastPass:** *https://lastpass.com/*

Use Whole-Disk Encryption

Stealing your computer is easier than hacking into it. OS X has built-in whole disk encryption that comes with virtually no performance overhead, especially if you have an SSD hard drive.

To enable it go to System Preferences/Security & Privacy.

From there open FileVault:

You can turn on FileVault and it will begin to encrypt your disk. It is best to let this happen overnight so that it is finished when you awake. Note: Your user account password will be used to derive the disk encryption key. It is therefore imperative that your user password is highly secure. Try to choose one that consists of a long sentence, ten words or more. For example, the password "f%L:7z123" is less complex than the password "I like to eat a burrito on a sunny day in June", however it could be argued that the latter is easier to remember.

Don't Use Your Work Laptop For Personal Purposes

This should go without saying, but… If you surf warez, porn, or torrent websites you are far more likely to be the victim of opportunistic attack. Rather than simply advising that you "don't do this", it is more realistic to advise "if you must do this:"

- Visiting such sites is best done in a Virtual Machine that does not persist file system changes. Google "vmware non persistent" for further information on creating VMs for dangerous pursuits.
- Do not do this on any computer you care about.
- Follow all of the advice in this document within the VM, too.

Don't Ignore Conventional Wisdom

With a reduced attack surface, limited scope for damage, and changed browsing habits, your browser will be significantly more protected should it ever come under attack.

Of course, there is still a lot to be said for security patches, anti-virus, and sensible Internet habits. Just make sure these things are your first line of defense, not your last.