SECURITY

Security & Privacy Settings for Apple Devices

This document prepared March 2015 for Alameda MUG

DATA·EX·MACHINA

FILEMAKER SERVICES

info@dataxm.com

STEPHEN HUSTON

Security Settings for iOS 8

Controlled from the Settings App

This will be the starting point for almost all iOS Settings.

Most of these settings do not have any significant effect on Security or Privacy, so we will note those which do deserve attention, and review those on the next 5 pages of this document.

The initial Settings screen is shown in 2 elongated columns; it is scrollable as a single screen in iOS 8, with the final section for Installed Applications at the end, expanding based on the actual apps installed on each device.

We will focus on these settings, which directly affect privacy and security:

Wi-Fi

Bluetooth

Cellular

Personal Hotspot

Notifications

Control Center

General (which controls Auto-Lock time)

Wallpaper (useful, if you care to use it)

Touch ID & Passcode

Privacy (and Location Services_

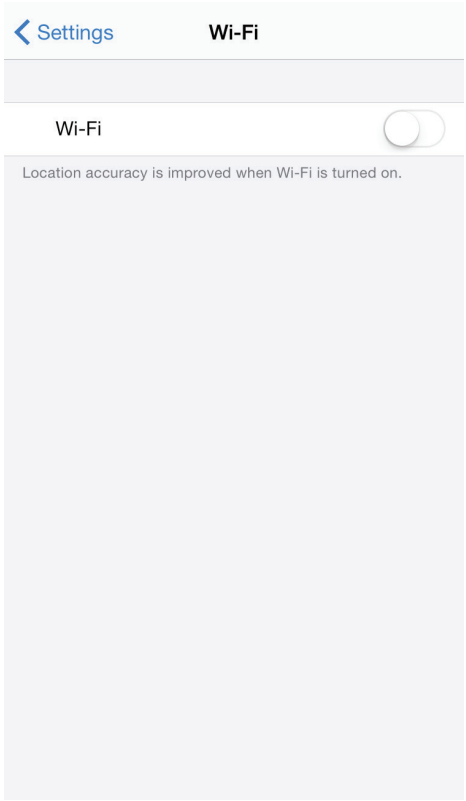
iCloud

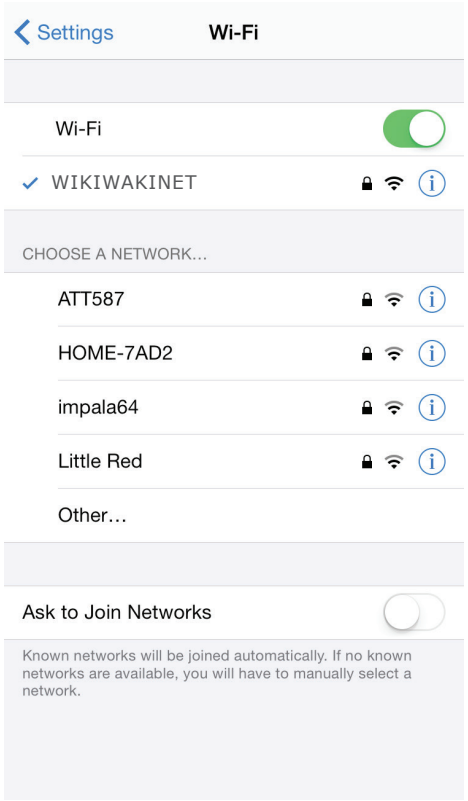
Safari

Mail, Contacts, Calendars — remove accounts you don't use on the device

Simple Rule-of-Thumb for iOS Settings:

Turn OFF everything you don't actually need to have ON.





Wi-Fi

Our basic rule says turn it OFF if you aren't using it.

When you turn it ON, it will be trying to connect to any network it recognizes from past connections, any unlocked network, and, if it can't find either of those, it will keep scanning and burning power.

If you use the circled "i" button next to a network, it will provide some info on that network, and give you the option to "Forget" it, which you should do with any network to which you do not want to connect automatically in the future.

Remember that, when you are connected to a network, your device and activity may be monitored by whoever is running that network, and by others on that network, including other patrons of a public network.

Bluetooth

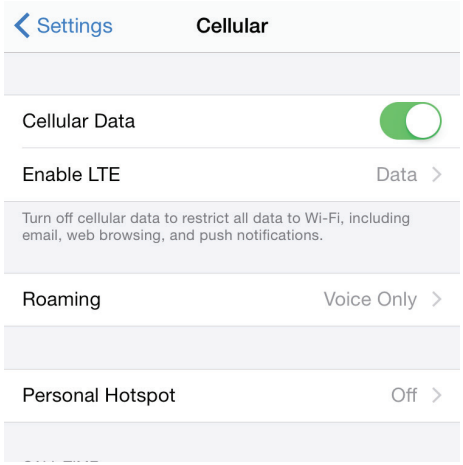
As with Wi-Fi, OFF unless you are actively using your device with a Bluetooth device. Otherwise other bluetooth-enabled devices including computers may be able to see your iOS device on a local bluetooth network.

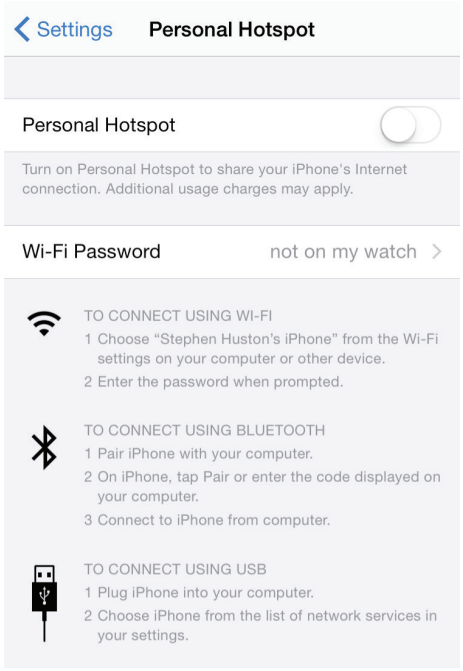
Cellular

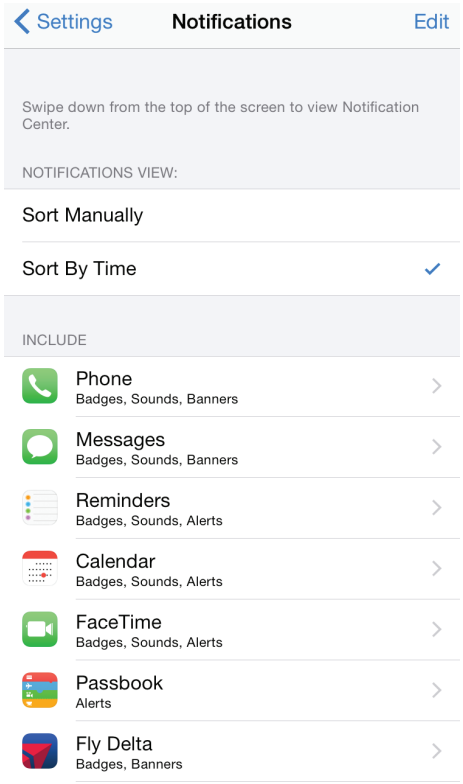
You need this ON for your phone to work, and this is also where you control your Personal Hotspot.

Leave the Hotspot OFF unless you are using it yourself, in which case give it a password with sufficient strength to keep others from using it.

Do not use any Default password which it suggests!



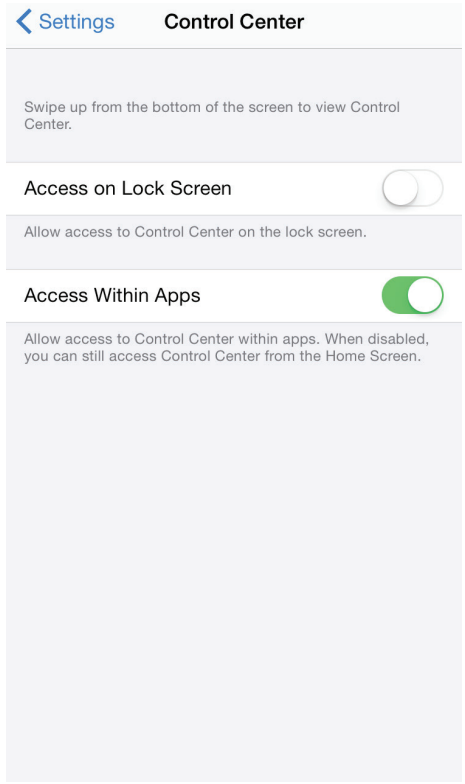




Notifications

This stuff may appear on your lock screen, and may even be useable from the lockscreen for some of the Apps without having to unlock the device. So be sure you only enable those items you need to see when they decide to tell you something.

Turn Off notifications from Apps you would ignore anyway. It just leaves a security hole that someone else might be able to use if they get hold of your device.

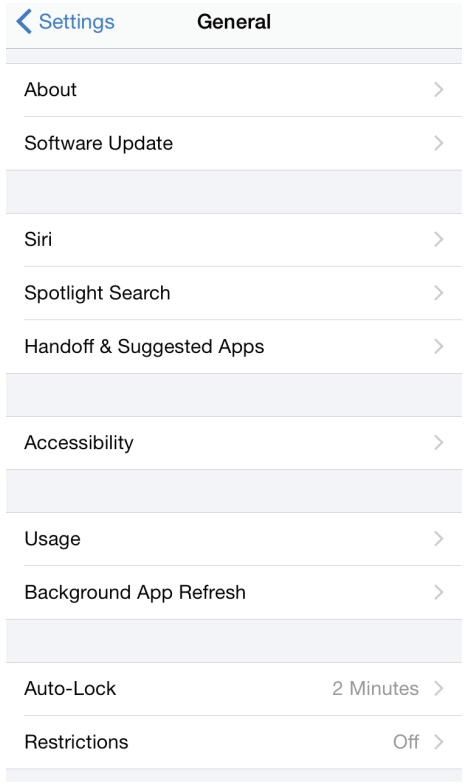


Control Center

Turn OFF access from the Lock Screen if you have Touch ID or can stand to enter your passcode to get at it.

Leaving it ON in Lock Screen enables anyone who handles your phone to turn off the radio signals which allow finding your device if it is lost or stolen!

Access from within Apps is fine, as you've already unlocked your device to get into the application.

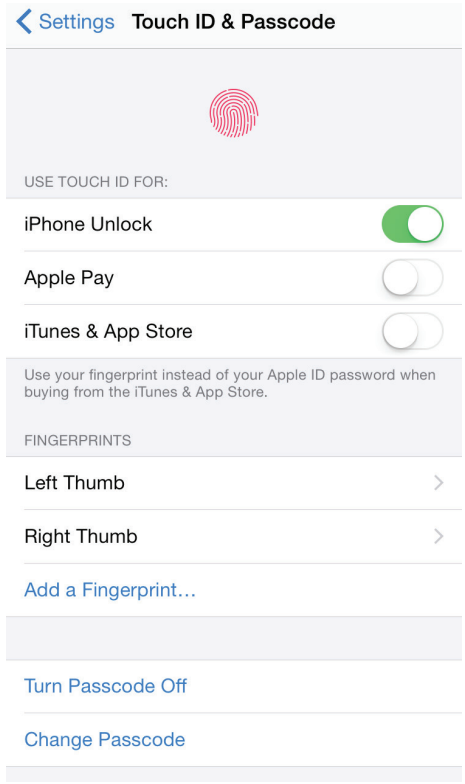


General > Auto-Lock

Auto-Lock should be ON and set to as short a time length as you can stand.

This controls when your phone will turn itself off and revert to the Lock Screen after you have quit touching its screen.

This also controls how long a thief would have to do anything they want if they grab your device off the table or even out of your hand while you are using it!

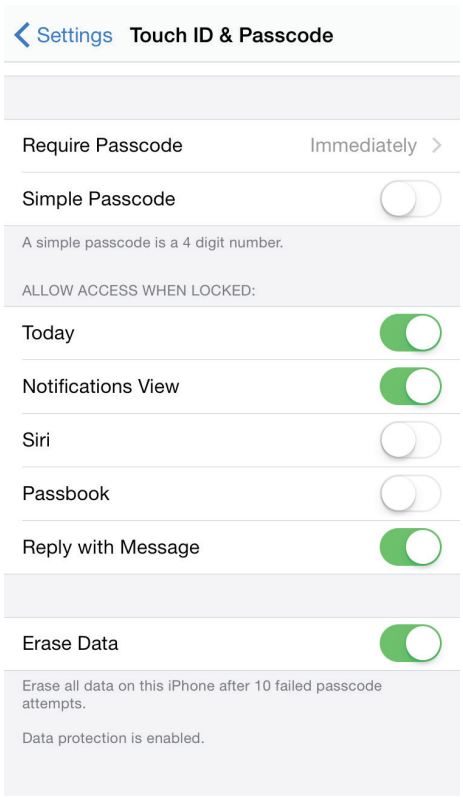


Touch ID & Passcode

Setup Touch ID if your device supports it, as the fastest way to unlock the device and reach the Control Center. Name your fingerprints in case one quits working,

Never allow the *Turn Passcode Off* option. An unprotected device is as good as gone, along with everything you had on it (email).

See the next page for the Passcode settings you'll see as you scroll down this screen…



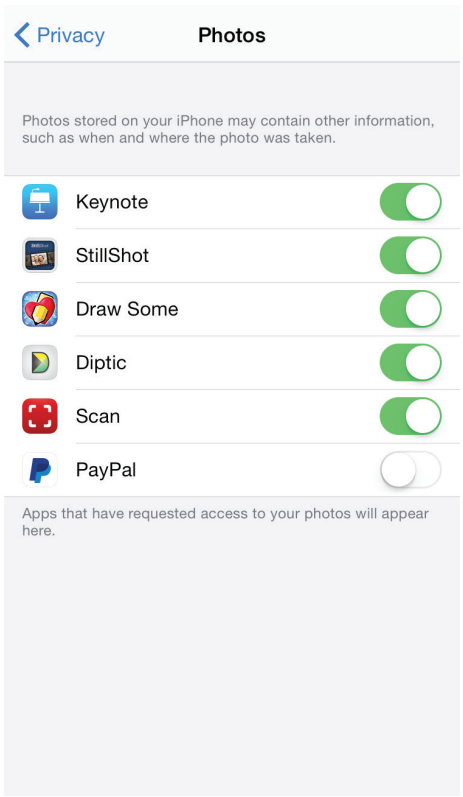
Touch ID & Passcode...

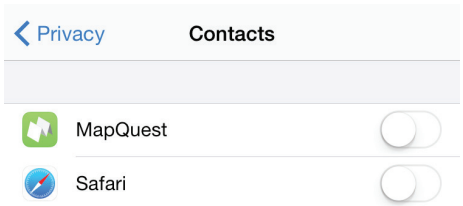
Require the passcode *Immediately* when the device locks.

Turn OFF the Simple Passcode. This changes the easy 4-number passcode to any length, which makes it harder to guess.

Allow those Notifications you setup in Notifications (earlier), and Reply with Message, to msg with if lost.

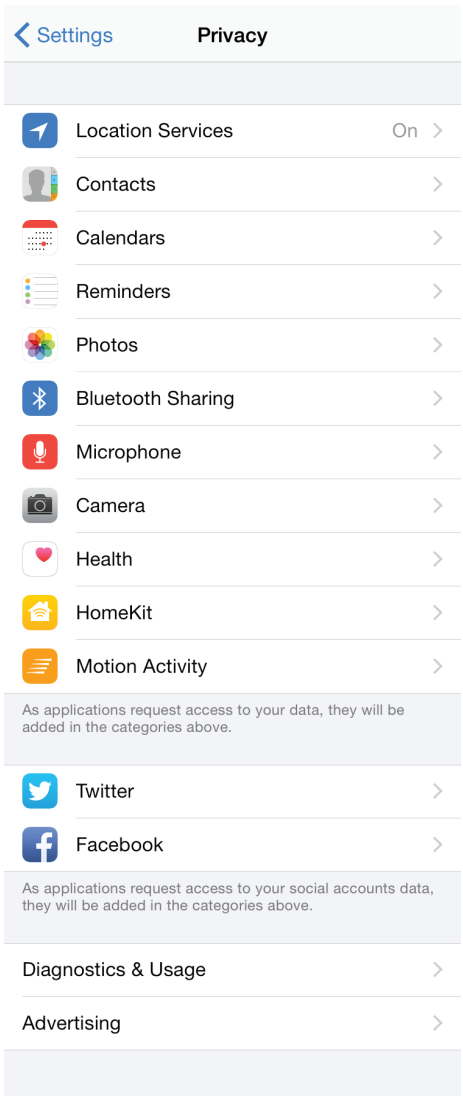
Erase Data = ON to erase your stuff if the passcode is misentered repeatedly by someone else.

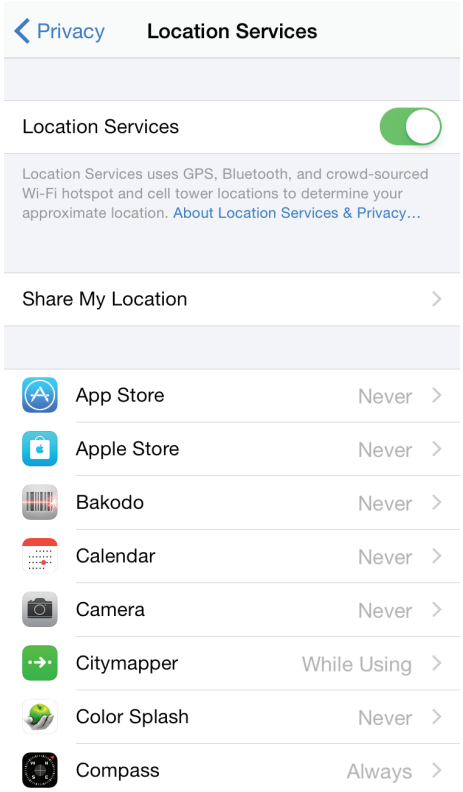


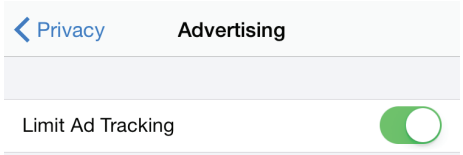


Privacy

Turn OFF all App access that's not useful to you, regardless of default. Don't give Apps access for which you can see no use other than to collect data.



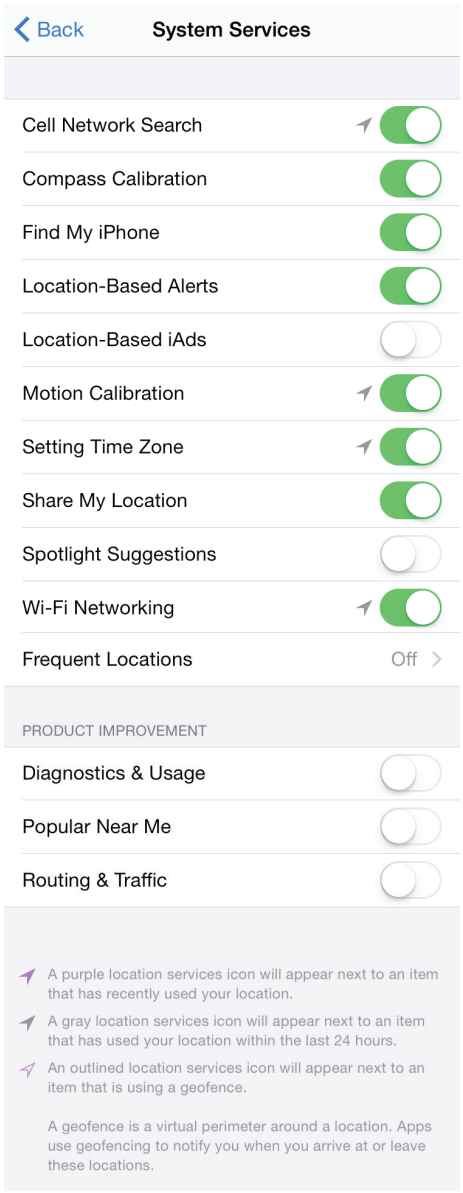




Location Services

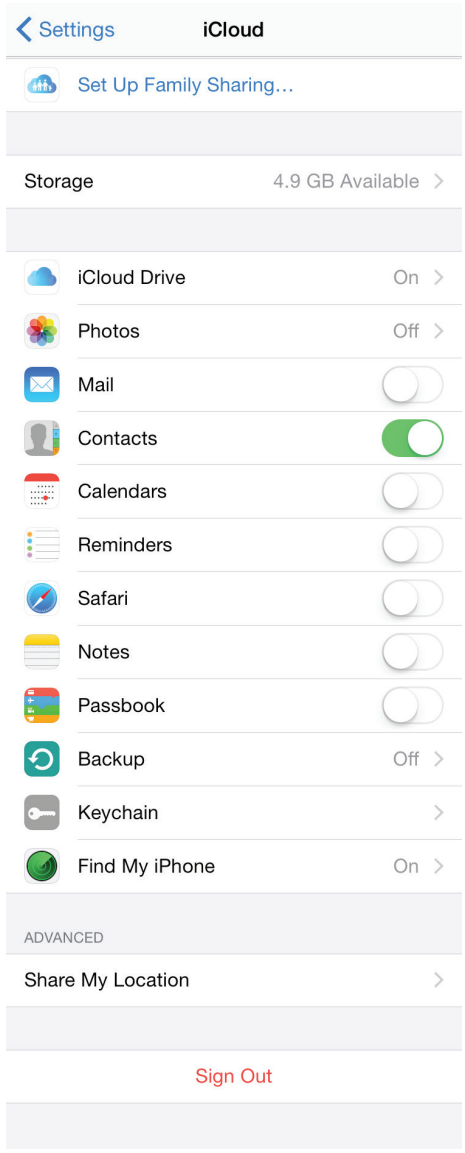
Turn OFF for Camera to stop embedding location where taken.

Set to Never except where you can pick "While Using" unless "Always" is appropriate.



System Services

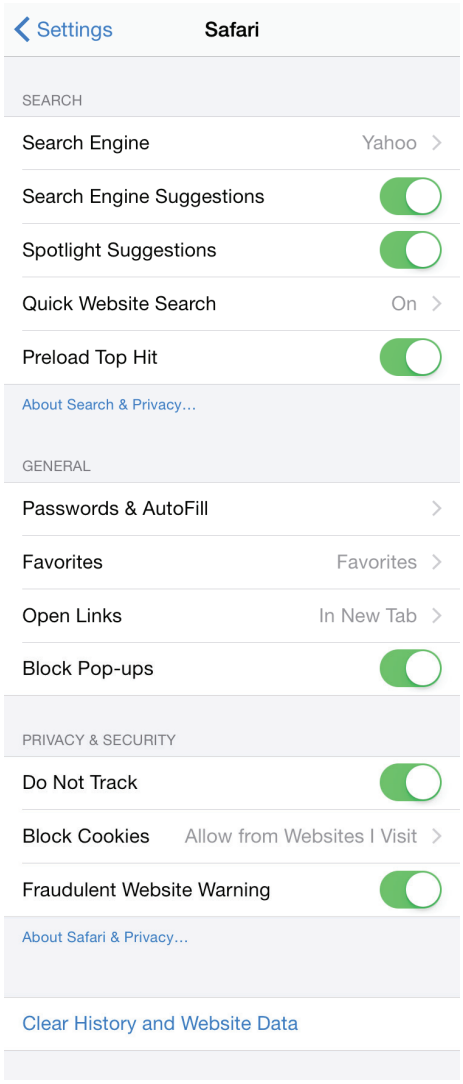
Turn OFF things you don't see any use for. Diagnostics and Usage may send info about your device to developers instead of to Apple.



iCloud Settings

Turn OFF everything you are not actually using.

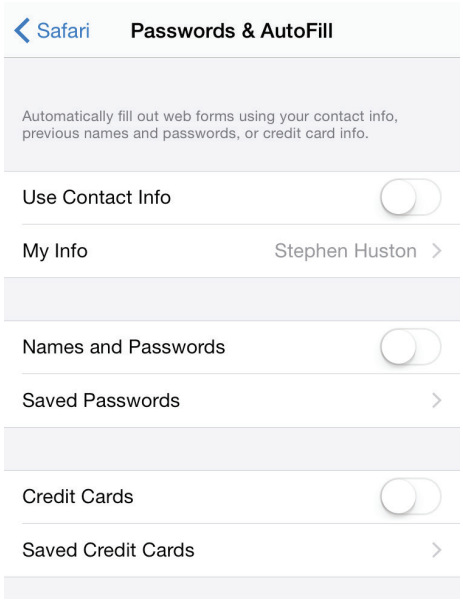
Find My iPhone/iPad = ON



Safari Settings

I block Pop-ups and set all of the Privacy & Security items ON.

Clear History & Data occasionally.



Safari > Auto-Fill

I recommend turning OFF all Auto-Fill options, including saved passwords.

Security Settings for OS X Yosemite

Controlled in System Preferences

Most System Preferences do not have any significant effect on Security or Privacy, so we note those which do deserve attention, and mention the key settings.

Simple Rule-of-Thumb for System Preferences:

Disallow everything you don't actually need to have enabled for the functionality you need.

Security & Privacy:

> General: Require a Password to unlock the screen after 5 seconds.

> Firevault: If you have sensitive data, encrypt your disk.

> Firewall: Enable it with the default settings. You can always adjust settings or turn it off if it hinders your activities.

> Privacy: Disable everything for which you don't know a need. You can always turn something on later if necessary.

Notifications: Turn off Lock Screen notifications for any Apps you don't intend to respond to immediately.

iCloud: Enable only those items you are actually syncing to multiple devices. Keep the rest local on your local drive(s).

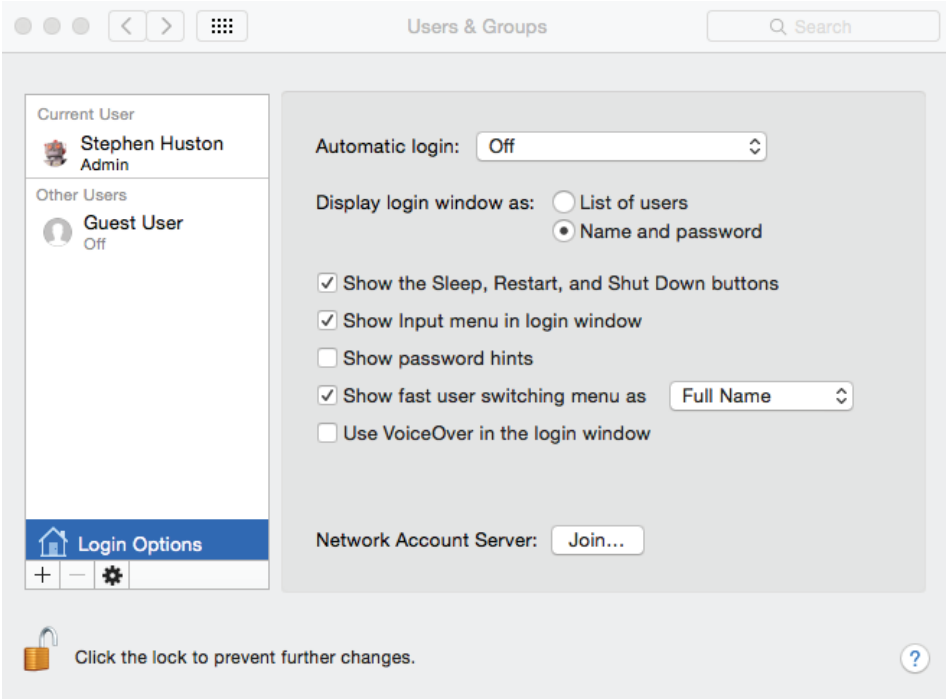
Internet Accounts: Setup only what you will use, and don't store account info unnecessarily.

Extensions: Know what they are, or find out. Don't let applications add Extensions to your system without researching them.

Network: Preserves network settings you have used. Clear out obsolete or unknown items.

Bluetooth: Be sure it is OFF unless you use it.

Sharing: Turn OFF all sharing from your local computer unless you know why it is ON.



Users & Groups: (above) Set the Login Options to require users to enter *both* their own Name and Password, rather than supplying half of the credentials they need to login via a list of valid user names. And don't give every user Admin authority unless you want them to change anything they want in the system for any other user(s).

Parental Controls: Allows restricting by application and content type.

App Store: Don't have the App Store set to check and download stuff without you being involved. Not all updates are equally good, not do you know what they may do to your system.

Time Machine: Think about "Backups" in case you need to replace a stolen computer. Where will your backup be?

The little lock icon in the lower corner of the System Preferences panels let you lock the settings so an Administrator's password is required for changes.

Security Settings for Airport Wi-Fi Networks

Settings in the Airport Utility application which is located at

Applications > Utilities

(You'll need to download or install this utility if it's not on your system.)

Open the Airport Utility and click on the Airport logo in the lower part of the screen, then click edit on the details which appear.

You will have to enter your password for the Airport Setup, which **SHOULD BE DIFFERENT** than your Wi-Fi network password. You don't want network users to be able to change your network's settings!

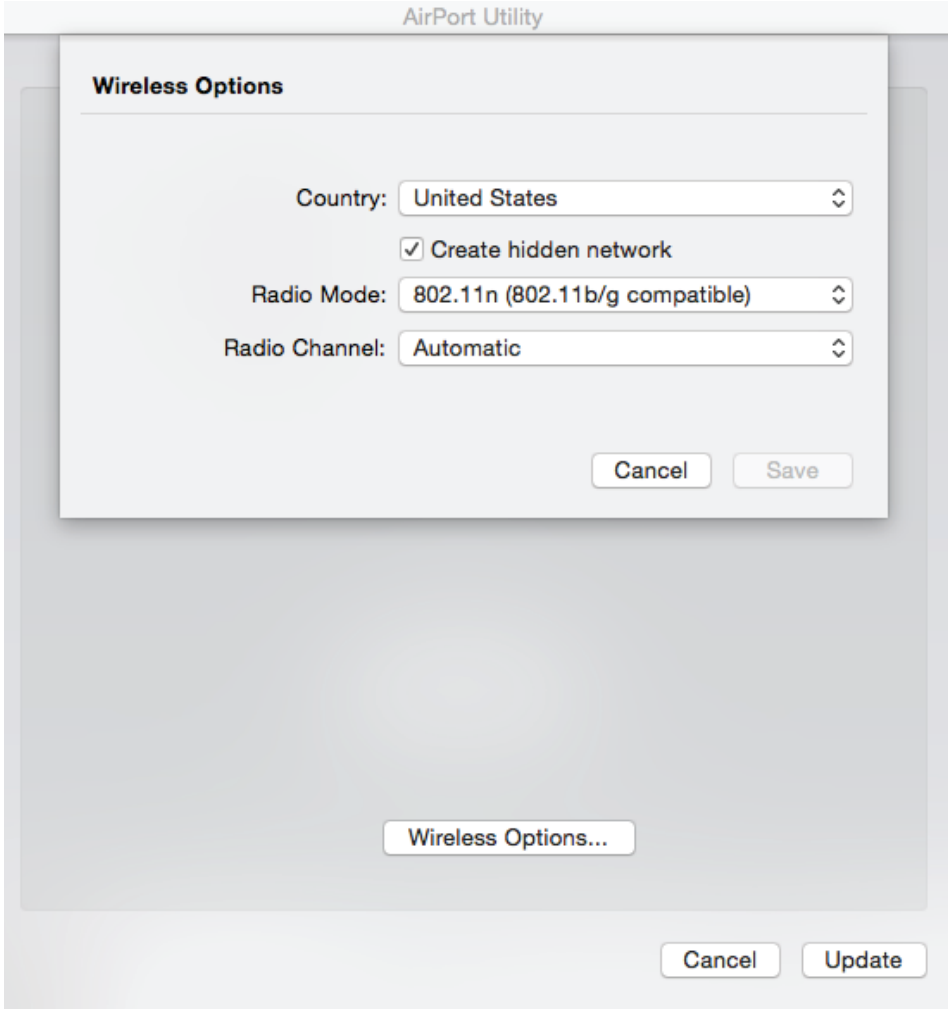
Choose **WPA2** security for your Wi-Fi — it adds network encryption.

Set a strong but easy-to-enter password for the wireless network so it cannot be guessed but won't take forever to type on an iOS screen.

Under the Wi-Fi tab, Enter a Name which can be typed simply on any device, but not one that will be guessable, nor any default name that the device suggests itself.

Then click the Wireless Options button at the bottom of that tab, and set the network name to be hidden with the checkbox: Create hidden network.

That way, only people who know the network's name can try to join it, instead of it appearing in a list of known networks to try to join or crack.



Password Resources

The website for evaluating time to complete a brute force cracking of a password is at:

https://www.grc.com/haystack.htm

The password cartoon regarding ***Correct Horse Battery Staple*** is at:

http://xkcd.com/936/