November 2016
Vol. XXVII, No 10

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ http://www.keystonemac.com

A Bunch of Things to Keep Your Computer Nimble

This month we have a variety of topics to cover. We plan to cover more of the new Sierra (macOS 10.12,) a couple of alternative browsers (Brave & Vivaldi,) and how to reindex you hard drive (something that could speed up your older, well-used computer.) We will also discuss alternative DNS servers. In light of the recent attack that crippled the internet, this last will be worth delving into.

Meet us at

Bethany Village Retirement Center
Education Room
5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, November 15 2016 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

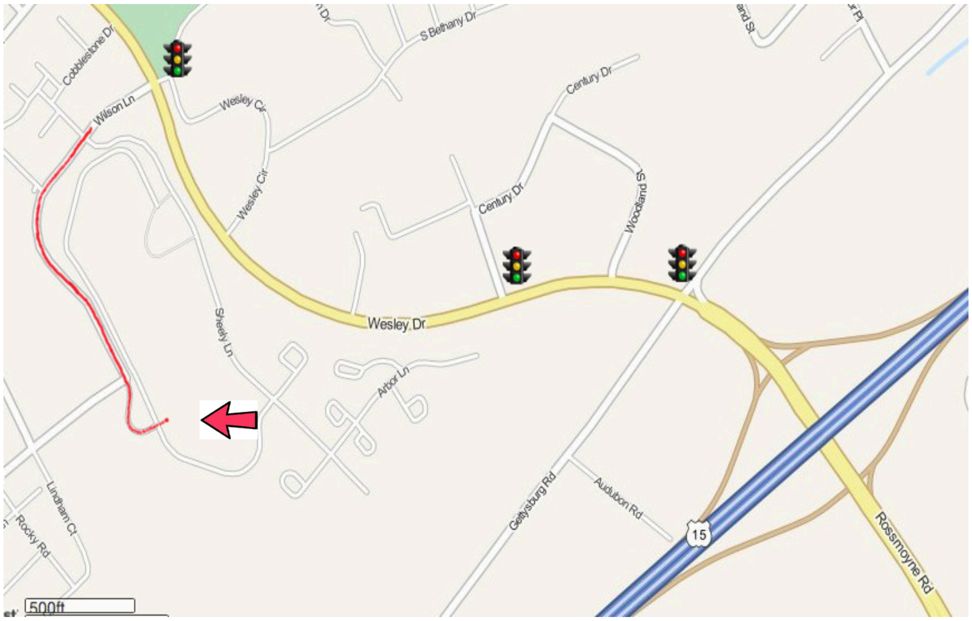
Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2016, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles form the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors



Keystone MacCentral Essentials

Meeting Place
Bethany Village West
Maplewood Assisted Living (Bld 21)
5225 Wilson Lane
Mechanicsburg, PA 17055

Web Site
http://www.keystonemac.com

Mailing Address
310 Somerset Drive
Shiresmanstown, PA 17011

by Josh Centers

Be Careful When Buying Apple Accessories on Amazon

Amazon may be the most popular online retailer in the United States, known for its low prices, fast shipping, and excellent customer service. But the company has a serious issue with counterfeiting.

In July 2016, CNBC reported on rampant counterfeiting of name brands by third-party Chinese sellers. The problem caused sandal maker Birkenstock to walk away from Amazon entirely.

Then, in August, Amazon tried to put a stop to counterfeit goods by making third-party merchants pay a $1500 fee to sell major-brand products. However, that requirement apparently hasn’t helped much, since Apple is now taking legal action against Amazon supplier Mobile Star, claiming that nearly 90 percent of Apple-branded accessories sold on Amazon are fake.

This lawsuit isn’t just a matter of Apple being offended. Using these cheaply made knockoff accessories can result in all sorts of problems: poor performance, electric shocks, and even fires and explosions.

Unfortunately, it can be tough to identify counterfeit products. Price isn’t necessarily an indicator, since the knockoffs are often priced the same as legitimate Apple products to aid in the deception.

While Amazon has been complicit in allowing counterfeit products to be sold, Amazon itself hasn’t been selling fakes. Rather, it’s third-party merchants selling via Amazon who are foisting the phony products off on customers. For that reason, some people have recommended steering clear of the “Fulfillment by Amazon” program that merchants can employ to have their products stored in and shipped from Amazon’s warehouses. That’s easier said than done, since so much of Amazon’s inventory comes from those third-party sellers. Personally, I haven’t had any problems with such products. I prefer Anker’s PowerLine+ Lightning cables to Apple’s, and Anker sells them directly via Amazon.

Another tip-off can come from reviews. TidBITS publisher Adam Engst was recently looking to buy an Apple Thunderbolt cable that looked entirely legit, but when he scrolled down to the reviews, a number of reviewers warned that they had received a counterfeit product. Reviews can be bought, so be sure to read a few of them, of various star ratings, before making a purchase.

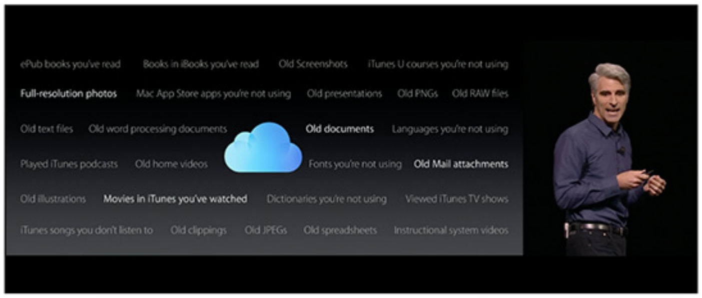
The only sure way to get authentic Apple products is to buy them directly from Apple, as Adam ended up doing with the Thunderbolt cable, or from an authorized Apple reseller.

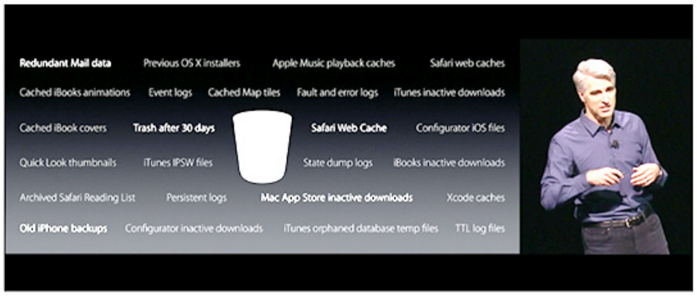
We hope that Apple’s lawsuit encourages Amazon to strengthen its anti-counterfeiting program. It’s bad enough to pay full price for knockoff sandals, but knockoff electronics can damage expensive equipment and cause injuries.

by Adam C. Engst

Explaining Sierra’s Optimized Storage

One of the marquee features of macOS 10.12 Sierra is Optimized Storage, a marketing term that Apple’s SVP of Software Engineering Craig Federighi introduced during the Worldwide Developer Conference in June (see “macOS 10.12 Sierra to Succeed OS X 10.11 El Capitan,” 13 June 2016). He described Optimized Storage as having two core functions, making room for new files by keeping old ones in the cloud and getting rid of files you’ll never need again.

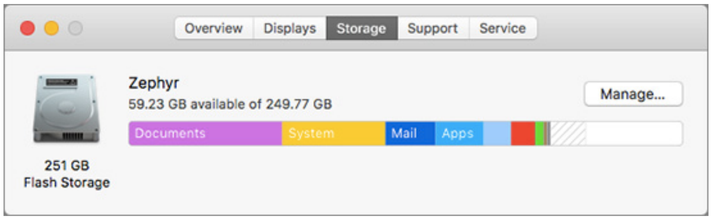




Federighi claimed that Apple took a representative Mac with 20 GB free on a 250 GB drive and "turned on all the switches" to clean out another 130 GB of space. For those struggling to free up space, particularly on a notebook Mac with relatively little internal flash storage, Optimized Storage sounded great, at least if you don't mind paying for online storage in iCloud Drive. And while it could be a great boon for such people, it turns out to be a somewhat confusing collection of seemingly unrelated features, burdened by one of the stranger interfaces that Apple has produced in recent years.

Plus, although we haven't had time to test all the possibilities, I recommend care when it comes to Optimized Storage in general, and extreme caution with one of its settings. That isn't to say you shouldn't enable all its features, but that you should understand the possible implications before doing so.

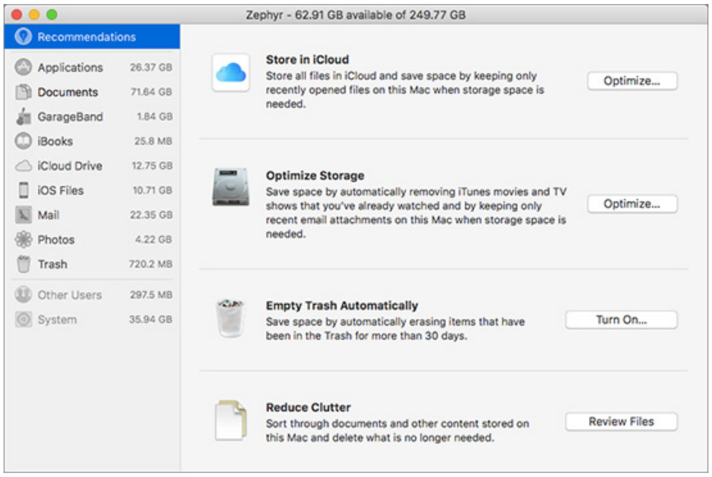
Accessing Storage Management — Before I get into the specifics of what comprises Optimized Storage, since you won't find that exact term anywhere in Sierra's user interface, let's look at how you access it. Choose > About This Mac, and click the Storage button. You'll see a stacked bar graph for each of your drives showing how much data of each type is on each drive — the categories include items like Apps, Documents, GarageBand, iBooks, iCloud Drive, iOS Files, Mail, System, Photos, and Other. At the end of the chart, you may see a hashed area that Sierra labels as Purgeable. Apple doesn't clarify what's included in Purgeable, but I suspect it comprises things like logs, cache files, and the contents of the Trash. Also new in this window is a Manage button.



Zephyr
59.23 GB available of 249.77 GB

251 GB
Flash Storage

Click Manage to bring up the centralized dashboard for Optimized Storage. In a truly odd interface decision, Apple chose to let you turn on Optimized Storage features from within the System Information app, rather than a pane of System Preferences, where nearly every other system-level setting resides. You can also bring up this window directly within System Information by choosing Window > Storage Management. The main thing to realize about the Storage Management window is that it's more of an assistant than a control panel — you can enable Optimized Storage's settings here, but what you see depends on what other settings you've selected, and you can't turn off or adjust any settings here. You do that in completely different parts of Sierra's interface.



Zephyr - 62.91 GB available of 249.77 GB

Applications	26.37 GB
Documents	71.64 GB
GarageBand	1.84 GB
iBooks	25.8 MB
iCloud Drive	12.75 GB
iOS Files	10.71 GB
Mail	22.35 GB
Photos	4.22 GB
Trash	720.2 MB
Other Users	297.5 MB
System	35.94 GB

Store in iCloud
Store all files in iCloud and save space by keeping only recently opened files on this Mac when storage space is needed.

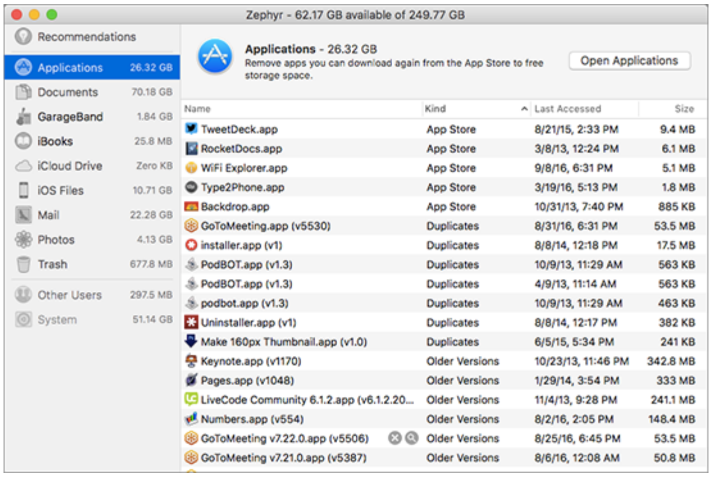
Optimize Storage
Save space by automatically removing iTunes movies and TV shows that you've already watched and by keeping only recent email attachments on this Mac when storage space is needed.

Empty Trash Automatically
Save space by automatically erasing items that have been in the Trash for more than 30 days.

Reduce Clutter
Sort through documents and other content stored on this Mac and delete what is no longer needed.

Managing Files Manually — The Storage Management window presents a familiar interface with a left-hand sidebar and large pane on the right that changes based on what you select in the sidebar. The top item, Recommendations, is where the most interesting stuff happens, and I'll explain its contents in a moment. But first, notice all the other entries in the sidebar, which correspond to the blocks of color in the About This Mac dialog's Storage view. For some app-based items, like GarageBand, Mail, and Photos, the Storage Management window merely gives you a button to open the app so you can manage its contents from within the app itself.

For a few app-based items like iBooks, and folder-based items like Applications, Documents, iOS Files, and Trash, Storage Management instead provides a Finder-like list view that shows each file's name, size, and last accessed date, along with kind for apps and documents. Click the column headers to change the sort, so you can focus on versions of similarly named files, see which files you haven't touched in years, or just look at them sorted by size.



Zephyr - 62.17 GB available of 249.77 GB

Applications	26.32 GB
Documents	70.18 GB
GarageBand	1.84 GB
iBooks	25.8 MB
iCloud Drive	Zero KB
iOS Files	10.71 GB
Mail	22.28 GB
Photos	4.13 GB
Trash	677.8 MB
Other Users	297.5 MB
System	51.14 GB

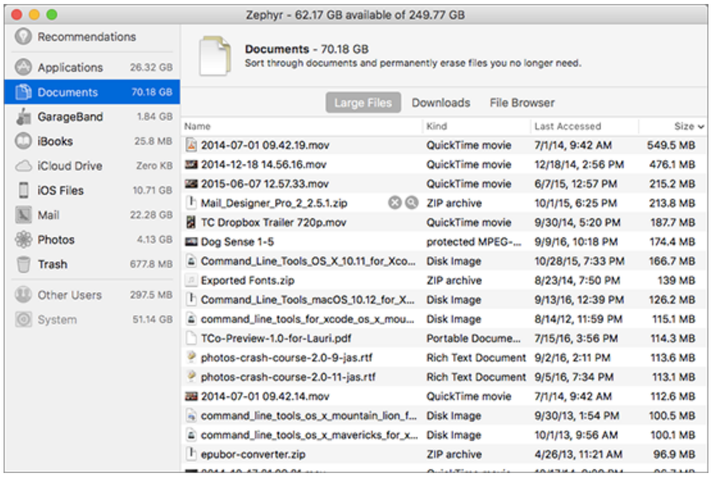
Applications - 26.32 GB
Remove apps you can download again from the App Store to free storage space.

Name	Kind	Last Accessed	Size
TweetDeck.app	App Store	8/21/15, 2:33 PM	9.4 MB
RocketDocs.app	App Store	3/8/13, 12:24 PM	6.1 MB
WiFi Explorer.app	App Store	9/8/16, 6:31 PM	5.1 MB
Type2Phone.app	App Store	3/19/16, 5:13 PM	1.8 MB
Backdrop.app	App Store	10/31/13, 7:40 PM	885 KB
GoToMeeting.app (v5530)	Duplicates	8/31/16, 6:31 PM	53.5 MB
installer.app (v1)	Duplicates	8/8/14, 12:18 PM	17.5 MB
PodBOT.app (v1.3)	Duplicates	10/9/13, 11:29 AM	563 KB
PodBOT.app (v1.3)	Duplicates	4/9/13, 11:14 AM	563 KB
podbot.app (v1.3)	Duplicates	10/9/13, 11:29 AM	463 KB
Uninstaller.app (v1)	Duplicates	8/8/14, 12:17 PM	382 KB
Make 160px Thumbnail.app (v1.0)	Duplicates	6/5/15, 5:34 PM	241 KB
Keynote.app (v1170)	Older Versions	10/23/13, 11:46 PM	342.8 MB
Pages.app (v1048)	Older Versions	1/29/14, 3:54 PM	333 MB
LiveCode Community 6.1.2.app (v6.1.2.20...	Older Versions	11/4/13, 9:28 PM	241.1 MB
Numbers.app (v554)	Older Versions	8/2/16, 2:05 PM	148.4 MB
GoToMeeting v7.22.0.app (v5506)	Older Versions	8/25/16, 6:45 PM	53.5 MB
GoToMeeting v7.21.0.app (v5387)	Older Versions	8/6/16, 12:08 AM	50.8 MB

Hover over any item and you see an X button for deleting the file and a magnifying glass button that reveals the file in the Finder. With these tools, Apple is trying to make it easier for you to delete large files you no longer need. You don't need to delete files one by one, either — just Command-click or Shift-click to select multiple files and press the Delete key to remove them all at once. You're given the combined size of all the selected files and warned before they're deleted, so you can use this technique to preview how much space a multi-file deletion will save.

The Documents view of Storage Management has three sub-views that help you focus on the task of clearing out unnecessary files, starting with the largest:

- Large Files, which on my MacBook Air lists files larger than 50 MB
- Downloads, which shows the contents of the Downloads folder
- File Browser, which provides a column view that's sorted by folder size and shows file sizes as well



Zephyr - 62.17 GB available of 249.77 GB

Recommendations	
Applications	26.32 GB
Documents	70.18 GB
GarageBand	1.84 GB
iBooks	25.8 MB
iCloud Drive	Zero KB
iOS Files	10.71 GB
Mail	22.28 GB
Photos	4.13 GB
Trash	677.8 MB
Other Users	297.5 MB
System	51.14 GB

Documents - 70.18 GB
Sort through documents and permanently erase files you no longer need.

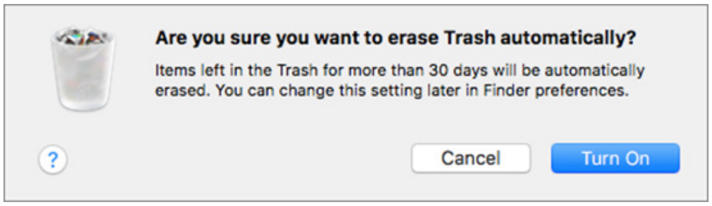
Name	Kind	Last Accessed	Size
2014-07-01 09.42.19.mov	QuickTime movie	7/1/14, 9:42 AM	549.5 MB
2014-12-18 14.56.16.mov	QuickTime movie	12/18/14, 2:56 PM	476.1 MB
2015-06-07 12.57.33.mov	QuickTime movie	6/7/15, 12:57 PM	215.2 MB
Mail_Designer_Pro_2_2.5.1.zip	ZIP archive	10/1/15, 6:25 PM	213.8 MB
TC Dropbox Trailer 720p.mov	QuickTime movie	9/30/14, 5:20 PM	187.7 MB
Dog Sense 1-5	protected MPEG-...	9/9/16, 10:18 PM	174.4 MB
Command_Line_Tools_OS_X_10.11_for_Xco...	Disk Image	10/28/15, 7:33 PM	166.7 MB
Exported Fonts.zip	ZIP archive	8/23/14, 7:50 PM	139 MB
Command_Line_Tools_macOS_10.12_for_X...	Disk Image	9/13/16, 12:39 PM	126.2 MB
command_line_tools_for_xcode_os_x_mou...	Disk Image	8/14/12, 11:59 PM	115.1 MB
TCo-Preview-1.0-for-Lauri.pdf	Portable Docume...	7/15/16, 3:56 PM	114.3 MB
photos-crash-course-2.0-9-jas.rtf	Rich Text Document	9/2/16, 2:11 PM	113.6 MB
photos-crash-course-2.0-11-jas.rtf	Rich Text Document	9/5/16, 7:34 PM	113.1 MB
2014-07-01 09.42.14.mov	QuickTime movie	7/1/14, 9:42 AM	112.6 MB
command_line_tools_os_x_mountain_lion_f...	Disk Image	9/30/13, 1:54 PM	100.5 MB
command_line_tools_os_x_mavericks_for_x...	Disk Image	10/1/13, 9:56 AM	100.1 MB
epubor-converter.zip	ZIP archive	4/26/13, 11:21 AM	96.9 MB

Other nice touches abound. In the Applications item, the Kind column shows you which apps came from the Mac App Store, which didn't, and which are older versions or duplicates that you can probably delete. I was surprised to find nearly 1.4 GB of old and duplicate apps on my MacBook Air. Notice too that different screens have different buttons, so Applications has a button to open the associated folder and Trash has an Empty Trash button. One thing you won't find is a graphical view like what GrandPerspective provides; nonetheless, I suspect that Apple's Storage Management interface will put a significant dent in the demand for utilities like CleanMyMac and Onyx.

But let's move on to the meat of Optimized Storage, as represented by the sections in Recommendations view: Store in iCloud, Optimize Storage, Empty Trash Automatically, and Reduce Clutter. I'll explain these in order of increasing complexity. Note that the wording (and even the icons) in this section changes depending on what options you may have already set. I've even seen it change multiple times as I'm watching, which is a horrible user experience. If it doesn't reflect what you believe it should, quit and relaunch System Information, open the Storage Management window again, and let it sit for a few minutes.

Reduce Clutter — I hesitate even to give this section a subhead since it's merely interface sleight of hand. All clicking the Review Files button here does is switch you to the Documents view so you can sort through and remove unnecessary files manually, as I discussed above.

Empty Trash Automatically — Moving up, the next section is Empty Trash Automatically, which is easy to understand. As it says, once a file has moldered in the Trash for 30 days, the Finder deletes it automatically, much like Photos automatically removes unwanted photos in its Recently Deleted folder after 40 days. Before this, files accumulated in the Trash until you emptied it manually, even if you ran out of drive space. I don't yet know if Sierra's Finder will offer to empty the Trash if you run very low on space.



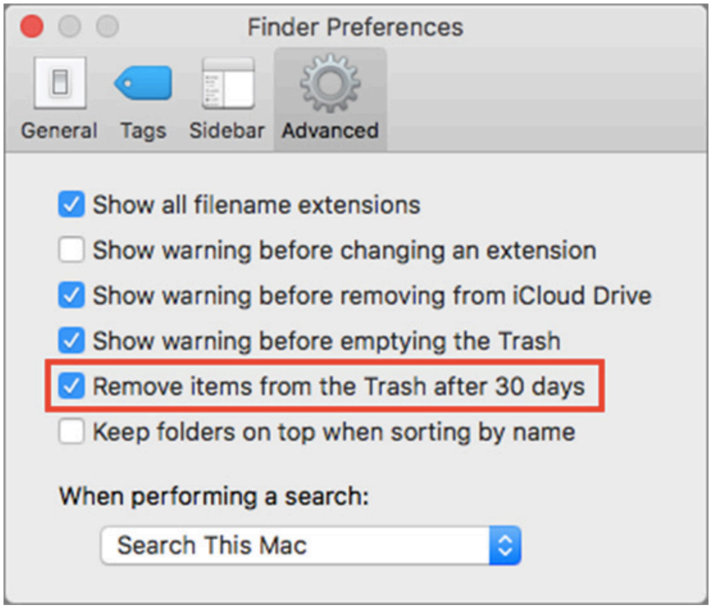
Are you sure you want to erase Trash automatically?

Items left in the Trash for more than 30 days will be automatically erased. You can change this setting later in Finder preferences.

Amusingly, Microsoft Windows has been capable of automatically deleting files from its Recycle Bin at least since Windows 98, although back then it deleted older files when adding a newer file to the Recycle Bin caused it to exceed a user-specified size. I'm surprised it took Apple this long to get to the point of taking the trash out for the user.

Whether or not you choose to enable this setting depends on what sort of person you are. If you can't stand the concept of wasting space — even space you don't need — on the contents of the Trash, you're probably emptying it manually all the time now. Automatic deletion of trashed items after 30 days likely won't scratch that itch for you. However, if you, like me, almost never empty the Trash unless you start to run low on drive space, I recommend turning on Empty Trash Automatically to help keep your Mac's drive from getting too full. It's a bad idea to let your drive fill up since that can cause crashes, corrupted files, and even directory corruption.

This setting also appears in Finder > Preferences > Advanced as the "Remove items from the Trash after 30 days"

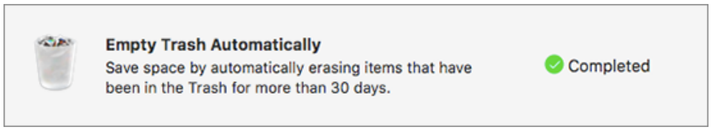


Finder Preferences

☑ Show all filename extensions
☐ Show warning before changing an extension
☑ Show warning before removing from iCloud Drive
☑ Show warning before emptying the Trash
☑ Remove items from the Trash after 30 days
☐ Keep folders on top when sorting by name

When performing a search:
Search This Mac

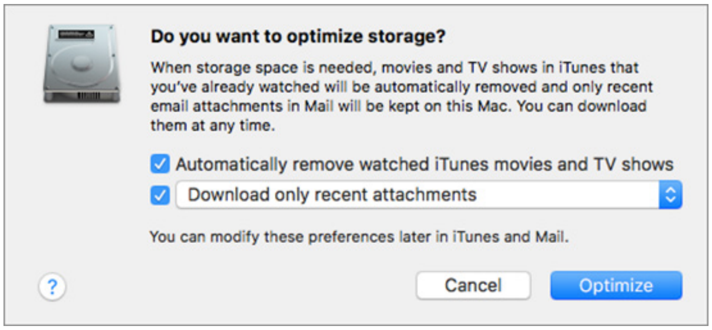
Should you ever wish to turn it off, you'll need to do that in the Finder Preferences, since enabling it in the Storage Management window replaces the Turn On button with a green Completed checkmark icon.


Empty Trash Automatically

Save space by automatically erasing items that have been in the Trash for more than 30 days.

Completed

Optimize Storage — Now we're getting into the confusing bits, starting with the fact that this aspect of Optimized Storage is called Optimize Storage (notice the missing "d"?). Clicking the Optimize button provides two options, one to automatically remove watched movies and TV shows and another to keep either only recent email attachments or no email attachments.


Do you want to optimize storage?

When storage space is needed, movies and TV shows in iTunes that you've already watched will be automatically removed and only recent email attachments in Mail will be kept on this Mac. You can download them at any time.

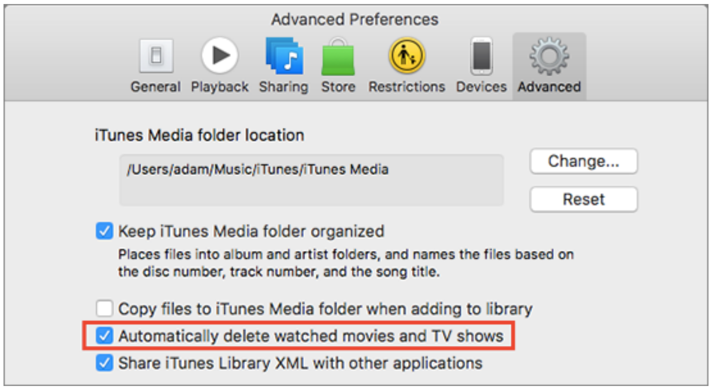
☑ Automatically remove watched iTunes movies and TV shows

☑ Download only recent attachments

You can modify these preferences later in iTunes and Mail.

Although I haven't been able to verify this for certain, I believe the Optimize Storage button affects only movies and TV shows purchased from the iTunes Store. When enabled, iTunes deletes watched movies and TV shows automatically, which is likely a good way to save a lot of space quickly, given the size of most video files.

Again, the Storage Management window of System Information only allows you to enable the Optimize Storage feature. To enable it directly within iTunes, or to turn it off if you want to make sure you can hold onto an already watched movie or TV show, go to iTunes > Preferences > Advanced, where you'll find a checkbox called "Automatically delete watched movies and TV shows."



iTunes Media folder location

/Users/adam/Music/iTunes/iTunes Media

☑ Keep iTunes Media folder organized

Places files into album and artist folders, and names the files based on the disc number, track number, and the song title.

□ Copy files to iTunes Media folder when adding to library

☑ Automatically delete watched movies and TV shows

☑ Share iTunes Library XML with other applications

Of course, you can always retrieve a deleted video in iTunes by choosing Movies or TV Shows from the Media Picker, clicking the Library button in the navigation bar, and clicking the Download button that looks like a cloud with an arrow coming out of it.

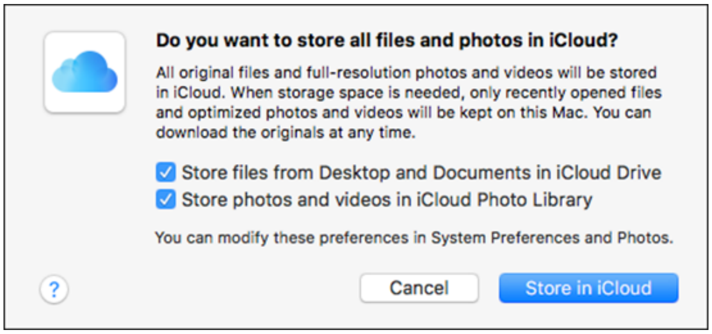
In an earlier incarnation of this article, I said that the email attachment feature had been removed in a late beta. That was wrong; the Storage Management window initially failed to present it to me, and to others, as an option, but after tweaking the feature in Mail manually, it returned.

To find that setting, open Mail > Preferences > Accounts > *acccount-name* > Account Information. There's a pop-up menu for Download Attachments that can be set to All, Recently, or None. The Optimize button in Storage Management gives you the choice of setting that menu to Recently or None for all your accounts; once set there, you can change it only in Mail's preferences.

There isn't that much new here; Mail has long had the option to not download attachments automatically (the Recently option is new). When you read a message with an attachment that's not downloaded, you can click its icon in the message to retrieve it. Apple hasn't said at what point Mail will consider an attachment no longer "recent," but I presume that it will at some point delete older attachments from the local mail archive such that you'd need to retrieve them again from the server.

Store in iCloud — The most confusing aspect of Optimized Storage comes in the first section of the Storage Management window, which is called Store In iCloud. The controls available in this section encapsulate two entirely separate features in Sierra, and worse, even the wording and checkboxes change depending on what you've already done.

On a Mac that doesn't have iCloud Photo Library enabled, when you click Store In iCloud, you get a dialog that gives you two checkboxes, one that lets you turn on syncing for your Desktop and Documents folders and another that enables you to turn on iCloud Photo Library. If either of those features is already on, the dialog changes (in the second dialog, I have iCloud Photo Library enabled, so it focuses on Desktop and Documents folder syncing).

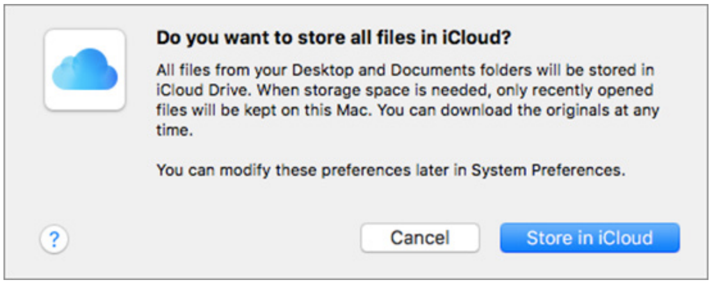

Do you want to store all files and photos in iCloud?

All original files and full-resolution photos and videos will be stored in iCloud. When storage space is needed, only recently opened files and optimized photos and videos will be kept on this Mac. You can download the originals at any time.

☑ Store files from Desktop and Documents in iCloud Drive

☑ Store photos and videos in iCloud Photo Library

You can modify these preferences in System Preferences and Photos.


Do you want to store all files in iCloud?

All files from your Desktop and Documents folders will be stored in iCloud Drive. When storage space is needed, only recently opened files will be kept on this Mac. You can download the originals at any time.

You can modify these preferences later in System Preferences.

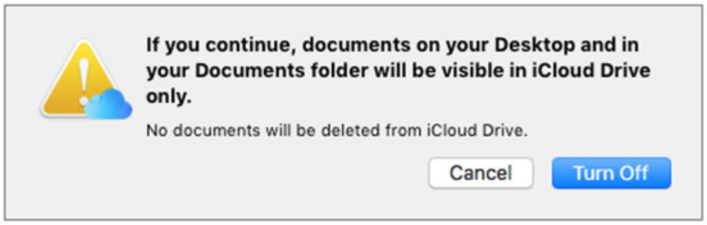
At this point, I need to explain Desktop and Documents folder syncing, a new feature in Sierra that's only peripherally associated with Optimized Storage. When enabled via the Storage Management window of System Information or the master switch at System Preferences > iCloud > iCloud Drive > Options, this feature moves your

Desktop and Documents folders from your home folder to iCloud Drive (itself a chimerical folder/volume). Don't look for them in your home folder because they're gone — I can't imagine why Apple didn't make symbolic or hard links to them in the spot where every user has been trained to look for them for the last 16 years. You can still access them from the sidebar in Finder windows, from the Finder's Go menu, or from within iCloud Drive.

The beauty of Desktop and Documents folder syncing is that as you enable it on other Macs using the same iCloud account, the contents of those folders on other Macs are merged via iCloud, so you end up with a single unified folder for Desktop and another for Documents. Even better, you can access the full contents of those folders via the iCloud Drive app on any iOS device signed in to the same iCloud account. It works well from what we've seen, but it may take some getting used to for those who have long maintained very different systems. I'm looking forward to using it to transfer screenshots made on one Mac to another automatically, since the Mac saves screenshots to the Desktop.

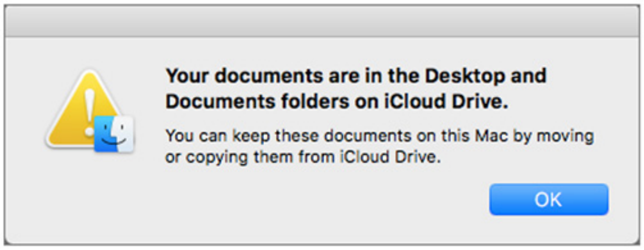
I have two warnings surrounding Desktop and Documents folder syncing. First, if you have gigabytes of data in one or both of these folders, you may have to start paying, or pay more, for storage space on iCloud Drive. The first 5 GB is free, and after that Apple offers several tiers from 50 GB to 2 TB. The storage space is shared with iCloud Photo Library, so if you're already paying for more to sync photos, you may have enough. But if you are going to start paying, it might be worth getting enough to use both Desktop and Documents folder syncing and iCloud Photo Library.

My second warning is that turning off Desktop and Documents folder syncing is stressful. When you do this, in System Preferences > iCloud > iCloud Drive > Options, Sierra tells you that all your files will be available only in iCloud, which seems wrong: if you're turning off syncing, you're doing so because you want them locally. However, that dialog is followed immediately by another that tells you that you can recover your files from iCloud Drive.



If you continue, documents on your Desktop and in your Documents folder will be visible in iCloud Drive only.

No documents will be deleted from iCloud Drive.

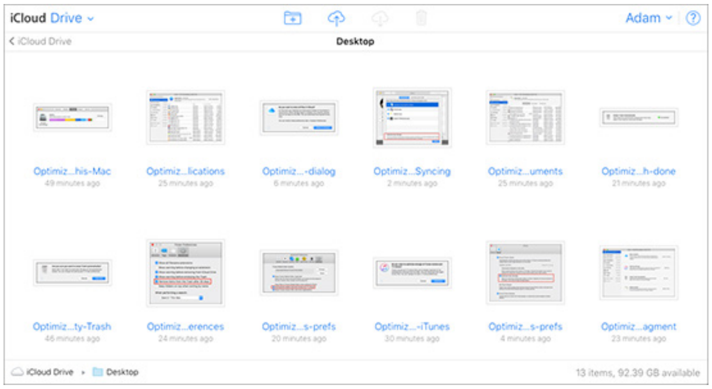


Your documents are in the Desktop and Documents folders on iCloud Drive.

You can keep these documents on this Mac by moving or copying them from iCloud Drive.

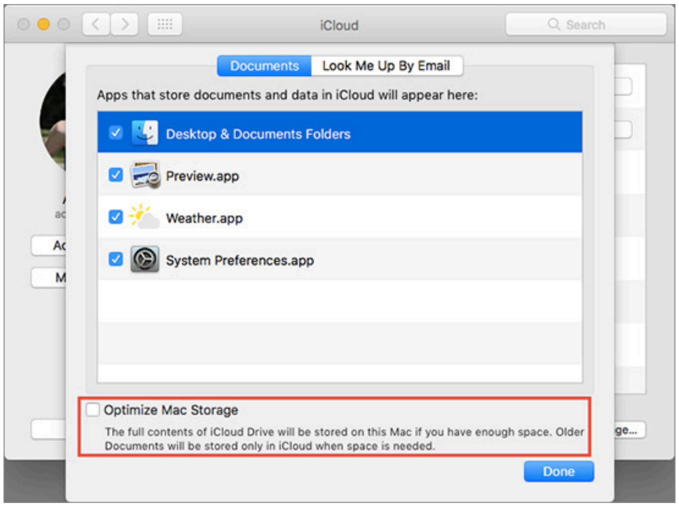
In fact, what happens when you turn off that feature is that Sierra recreates empty Desktop and Documents folders in your home folder. You can't replace those, so you can't drag the old Desktop and Documents folders from iCloud Drive to your home folder; instead, you must open each folder in iCloud Drive and *move* (Command-drag) its contents to the local Desktop and Documents folders in your home folder. You can try to delete the now-empty Desktop and Documents folders from iCloud Drive, but in my experience, iCloud keeps recreating at least the Desktop folder.

In general, if you ever turn off an iCloud Drive feature and seem to be missing files, restart your Mac and wait a bit. You can also check for the files on iCloud.com itself.



Trust in iCloud? — Now that you understand Desktop and Documents folder syncing, we can return to what happens when you enable the checkboxes that you get in the Storage Management window when you click Store In iCloud. The effect of clicking these checkboxes goes beyond just turning on Desktop and Documents folder syncing and iCloud Photo Library, and this is where Optimized Storage comes in again:

- With Desktop and Documents folder syncing, when you open System Preferences > iCloud > iCloud Drive > Options, there's a checkbox called Optimize Mac Storage. When selected, it allows Sierra to delete old, large files from your local drive to save space, leaving just a copy in iCloud Drive — you'll still see the icon in your Finder, but it will have a cloud badge on it, indicating that it's not stored locally. If that gives you the willies, you're not alone.



Apps that store documents and data in iCloud will appear here:

☑ Desktop & Documents Folders
☑ Preview.app
☑ Weather.app
☑ System Preferences.app

☐ Optimize Mac Storage

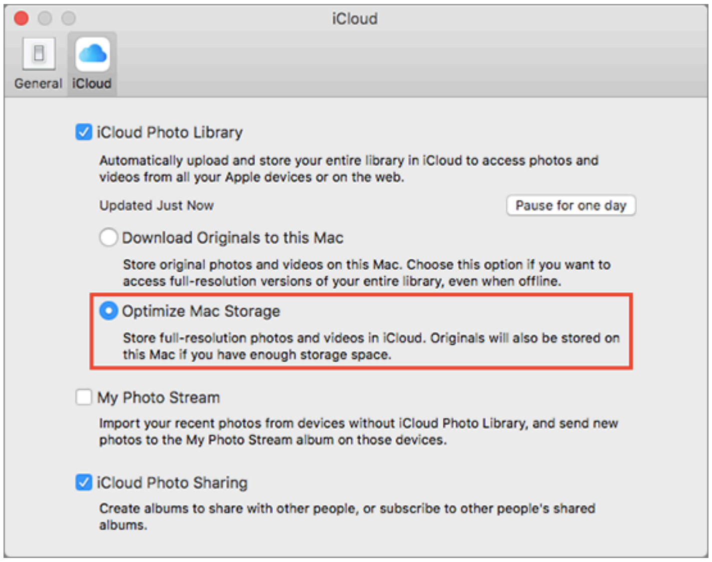
The full contents of iCloud Drive will be stored on this Mac if you have enough space. Older Documents will be stored only in iCloud when space is needed.

The question here revolves around backup. Let's say you turn on this feature, and it copies the contents of your

Desktop and Documents folder to iCloud Drive. Time passes, and some old, large files in your Documents folder are deleted from the local drive to free up space. They still exist in iCloud Drive, appear on your local drive as stubs that you can click to download, and in any local backups created before they disappeared from your local drive. Now imagine that your backup drive dies, and you need to create a new backup. Will those old, large files be downloaded from iCloud Drive and backed up? Or will the version in iCloud Drive be the only extant copy?

I cannot currently recommend selecting this Optimize Mac Storage checkbox. It will take time to test what happens with backup strategies when Optimized Storage starts deleting files, and since you presumably have sufficient space on your Mac now, it's better to be safe than sorry.

- With iCloud Photo Library, selecting the checkbox in Store in iCloud also selects an Optimize Mac Storage radio button in Photos > Preferences > iCloud. That has the effect of storing full-resolution photos and videos in iCloud and only keeping them on the Mac if there's space. (When you work with an item whose full-resolution original is in iCloud, Photos downloads it first.)



☑ iCloud Photo Library

Automatically upload and store your entire library in iCloud to access photos and videos from all your Apple devices or on the web.

Updated Just Now

○ Download Originals to this Mac

Store original photos and videos on this Mac. Choose this option if you want to access full-resolution versions of your entire library, even when offline.

● Optimize Mac Storage

Store full-resolution photos and videos in iCloud. Originals will also be stored on this Mac if you have enough storage space.

□ My Photo Stream

Import your recent photos from devices without iCloud Photo Library, and send new photos to the My Photo Stream album on those devices.

☑ iCloud Photo Sharing

Create albums to share with other people, or subscribe to other people's shared albums.

There's nothing new about this iCloud Photo Library setting; it has been in Photos since the launch of iCloud Photo Library. In the past, however, you had to enable Optimize Mac Storage manually, and we have firmly recommended that you never enable it on your primary Mac, where you presumably have sufficient drive space for your entire photo library. Optimize Mac Storage is great for a MacBook Air that lacks room for all your photos, but in our view, you should always have a full local copy of all your photos, backed up on local storage.

In the end, the question comes down to whether or not you trust iCloud, because once you enable these features, iCloud becomes the "truth," in the lingo of syncing. That's fine if you have local copies and local backups to restore from should something horrible happen to iCloud or your account, but in both of these cases, it seems theoretically possible that you could end up with no local copies at all. If you're not all that attached to your data, or if you're willing to cede all responsibility for your data to Apple, that may be acceptable. Personally, I want to know that I have a copy of every document and photo stored locally on at least one Mac and backed up locally in at least one spot.

During WWDC, Craig Federighi said that Apple has over 10 billion documents in iCloud today, although I wonder if that number includes photos or reflects mostly iOS storage, given how few people I see using iCloud Drive to store Mac documents. The problem is that I've heard too many stories about people experiencing problems with data stored in iCloud to trust it implicitly. I'm not perturbed about iCloud security in particular; Apple makes all the right noises about iCloud security and privacy. But there's a big difference between having the right intentions and eliminating all bugs. iCloud is usually fine as a syncing service, but that's a far stretch from trusting it with the only copy of valuable data.

by Jeff Porten

On Hacking During the U.S. Presidential Campaign

Technology has been front and center of this year's presidential campaign, and not in a good way. We argued endlessly about Hillary Clinton's implementation of email while she was Secretary of State, we learned about the hack of the Democratic National Committee and other Democratic campaign organizations, and we were treated to the spectacle of a presidential nominee requesting a foreign government to release more stolen documents. Whether or not that request was sarcastic, it pretty much ensured that subsequent discussion would be devoid of technical detail in favor of campaign optics. I hope to rectify that situation somewhat.

I won't address the issues with Clinton's email server here for reasons of brevity, but also because the technical detail necessary to analyze the situation is not public. More information is available to evaluate the security considerations resulting from other hacks that have come to light.

The Three Circles of Computer Hackers — As a technology professional, I've been frustrated by the news focus on scandal versus actual security issues. Clinton's email server is endlessly debated and will likely be a topic of discussion long after the election if she wins. Meanwhile, few people are even aware that the State Department's email was definitely hacked, which certainly included far more email messages than were on her private server.

The Office of Personnel Management, the Internal Revenue Service, and potentially dozens of other government networks were also compromised, but these have been at best two-day stories in the mainstream press, followed by debate only in techie circles. When a hack has staying power in the mainstream media, such as the one suffered at the DNC, it's because it feeds partisan debate, and the technical issues are ignored.

Before we get into the details of the hacks, it's worthwhile to discuss who these hackers are. I classify them into one of three groups: script kiddies, lone hackers and criminal networks, and state actors.

- **Script Kiddies:** Most of the time, when you hear about a powerful hacker in the press, that person is actually a "script kiddie." Once a security flaw is discovered, and a corresponding hacking tool is developed, said tool has commercial value in the more disreputable corners of the Internet. "Script kiddie" was coined to describe the hypothetical 12-year-old who, with little knowledge of actual hacking, downloads such a tool and unleashes it from their home computer.

This is not a new phenomenon — I had a friend in high school who was visited by the FBI in 1985 and politely asked not to touch any computers for a few years. What is new is that these people can easily congregate on the dark web, enabling a security vulnerability to go from recently discovered to worldwide-attack-vector in hours.

Script kiddies use existing tools and known vulnerabilities; their target is the user who ignores security updates. (Don't be that person.) As such, script kiddies are easily defended against. However, they're also useful as political fodder when it's in the interest of an agency to report they were attacked over 70,000 times. It's not the quantity we should worry about, it's the quality.

- **Lone Hackers and Criminal Networks:** The real concern to most people are the hackers who discover new vulnerabilities and the criminal networks that exploit those vulnerabilities.

It's important to note that "hacking" itself is not a bad thing: it's just a kind of computer forensics and programming. "Black hat" hackers are the bad guys; "white hat" hackers are hired by businesses and governments to protect you. Black hat hackers often crop up in places where highly skilled technical people tend to be underemployed. Thanks to the Internet, it's trivial for these people to organize or be recruited by criminal organizations; when you hear about a hospital paying a $17,000 ransom to get its files back, that's whom they're paying.

Hackers are portrayed in movies as near-magicians, able to access just about any digital file on the planet. In reality, their abilities are much more limited but still pretty scary. The best defense against them, as with the script kiddies, is keeping up-to-date with security updates — you're relying on the computer industry to learn about potential vulnerabilities before the bad guys do. The Internet and many computer resources were built during a much more trusting era, and have evolved into an astonishingly complex system. As a result, the whack-a-mole process of "find a vulnerability and patch it" is what we'll have to live with for decades to come.

The Achilles heel of the black hat hackers and the criminal organizations that employ them is that they need to monetize their hacks: information, once discovered, has to be sold or exploited. This need provides an opportunity for law enforcement both to discover the hack and to trace its source. The best friend of these hackers is secrecy: corporations that cover up data breaches for fear of public embarrassment, technology companies that keep their source code secret (and unavailable for review by outside experts), and government agencies that don't publicize attacks for fear of exposing their vulnerabilities.

- **State Actors:** Here is where we really need to draw a distinction in hacking organizations. There are state-run hacking groups and everyone else. The technology that state-sponsored hackers have access to is secret, but we can guess several things. First, they have budgets larger than any available to all but the biggest criminal networks. Second, they have access to classified hardware and software that likely outstrips what's available on the mass market. Third, when they find a vulnerability, they can sit on it for years, harvesting exposed information without publicity. And fourth, they can work with friendly companies and old-fashioned spies to build backdoors and other vulnerabilities into the technology that's sold to the public and to other governments.

It's that last reason that helps make the scariest techies on Earth not "Chinese hackers" or "Russian hackers," but "American hackers." It's nearly certain that the most sophisticated and powerful cyberwarfare capabilities are those deployed by American agencies. Some of these technologies are defensive — as with anthrax, sometimes you need to possess a weapon in order to understand how to defend against it — but since a cyberweapon is covert in the way that a guided missile very much isn't, it's anyone's guess just what the U.S. government is doing with its cyberwarfare capabilities.

We do know that other governments are doing their best to catch up. The Chinese and Russian governments have dominated the headlines when it comes to recent attacks on American entities, but any country with a significant military capacity has a cyberwar component running alongside it. As the dominant nation when it comes to building new consumer-level computer hardware and software, it's likely we have an equivalent lead in covert military uses of similar technology.

The distinctions between these hacker types become important when you start asking the question of whether you personally are being targeted.

Script kiddies and individual hackers use scattershot methods to attack vast numbers of devices on the Internet; ergo, to stay safe, we should all employ basic security tools and practices (even if they're just built into our hardware, software, and services).

You're in more danger if you're targeted by a capable black-hat hacker or criminal network; they might hit you with attacks designed to penetrate your organization's defenses. Unless you're a high-level employee in a major company or someone with access to confidential systems, it's unlikely that you'd be targeted personally. However, individuals have been targeted for angering the wrong people, and hackers can be hired by a personal enemy. Most people are generally safe from personal attack, but there are exceptions.

If you're the target of a state-run hacking organization, all bets are off: it's impossible to know what tools state sponsored hackers might use to penetrate your systems, but the story behind Apple's recent iOS and Mac updates can give you an idea of what's possible (see "iOS 9.3.5 Blocks Remote Jailbreak," 25 August 2016). Governments may be interested in your activities for legitimate or political reasons; if so, constant vigilance on top of excellent security practices would be necessary.

Our Democracy Has Been Hacked — This brings us to the Russian attack on Democratic campaign organizations. That statement has already been politicized, as some people have tried to obfuscate who masterminded the attack.

Here's the evidence pointing to the Russian government: the Romanian hacker who claimed credit for the hack doesn't seem to be a native Romanian speaker; the series of events following the attack follows the pattern of Russian disinformation campaigns; and the signatures of the hack identified the perpetrators as two organizations known to work with and for the Russian government.

There are two ways in which this hack affects the election:

First, the last time foreign security agencies were interested, or actively involved, in influencing U.S. elections was when we were in an openly confrontational situation. Such activity is historically documented on both sides of the Cold War, but certain lines haven't been publicly known to be crossed since. Yes, other countries have tried to support American domestic political movements in the hopes of generating a friendlier government (to them). But as far as we know, they've rarely tried to support or torpedo specific candidates; the last time the Russians tried (unsuccessfully), they were called "Soviets" and we were locked in the Cold War.

Second, it means that literally thousands of political entities are now potentially being targeted by foreign agencies with significant capabilities. Your reaction to hearing of an attack on a national Democratic organization may have been horror or schadenfreude depending on your voting plans, but consider who really runs politics in America: a number of nationwide organizations, a hundred statewide entities (and a hundred more during a presidential campaign), and literally thousands of county and city groups involved in local politics.

Most of these people are volunteers who likely have average technical skills. What these volunteers don't have is access to computer security resources and training, unless they're provided by the national political organizations. And to the extent that security advice has been provided, we can presume that it was done with an eye toward preventing hacks by political opponents, rather than sophisticated state agencies.

I'm not trying to describe a conspiracy to subvert all elections, but the dangerously close ones are vulnerable. If Clinton's lead over Trump is substantial, it's unlikely that foreign influence would be enough to tip the election. But if it were to get closer, things could change. Most of us remember an election 16 years ago that was decided by 537 votes in Florida. In a close election (or even just in close states), outside tampering with the political process could be a deciding factor. I live in Philadelphia; if the local Democratic organization's computers were crashed here on Election Day, Clinton could have a substantial lead in Pennsylvania and still lose to Trump on a failed get-out-the-vote effort.

The Election Hack — Unfortunately, the attack on Democratic organizations isn't even the most recent in the news. Voter registration systems in Illinois and Arizona were targeted and penetrated to varying extents. It's important to note that it's unknown (or at least, not public) who is behind these hacks; we can't assume the Russians are also targeting our election systems. But somebody is.

The motive behind these hacks is also unclear. No registration data was changed in either case; in Illinois, 90,000 voter registration files were downloaded, so it could have been a matter of simple identity theft. Malware was installed on the Arizona server, but officials haven't reported what it was attempting to do. It's entirely possible that the intent of these hacks was purely criminal, not political.

That shouldn't make us relax, however. These hacks show that our election systems are vulnerable, and future hacks may try to sway elections. Not to put too fine a point on it, but our political system is not designed to defend against such threats. Elections are run by the fifty states, and implemented by thousands of city and county election boards. You might think that most Americans have an interest in, say, the integrity of elections in Georgia, which has 2 senators and 16 electoral votes; the state of Georgia, though, thinks you should mind your own business.

Beyond that, we're vulnerable because we have heavily politicized the debate over election integrity. Republicans routinely claim that voter fraud is rampant (despite evidence to the contrary), and Trump claims that fraud would be the only explanation were he to lose Pennsylvania. Democrats argue that this concern amounts to crocodile tears to provide political cover for disenfranchising groups who happen to vote Democratic.

I have my own opinions about which side is correct, but one thing is certain: the debate is so politicized that it was impossible to choose links that everyone would agree came from credible sources. I cited the Brennan Center because it's the first result in Google (after signing out and anonymizing my browser); for all I know, a significant percentage of my readers might have been told that the Brennan Center is unreliable by news sources they trust.

It's easy to be disappointed when your candidate isn't doing well in the polls or has lost a given state. It's a lot harder to give credence to claims of fraud and hacking attacks on elections when opening that can of worms might overturn a win by a candidate you support. For that reason, I expect post-election arguments about possible hacks to be driven entirely by partisan reaction, and to have nearly nothing to do with factual information. Even finding facts will be made more difficult amid the noise made by partisan bickering.

How the Thoughtful Voter Should React — Full disclosure: I'm a partisan Democrat. Like many of my political persuasion, I chortled mightily when I read about the impact of a failed computer system on the Romney campaign in 2012. But that was a self-inflicted wound. I would feel differently if that damage had been caused by outside agents, even if they were Democratic actors on "my side" attacking the system. I can't support winning an election by corrupting it. I would feel even more strongly that way if the hacking were done by a foreign government.

As a democracy, we need a reasonable expectation that our elections are, for the most part, the will of the populace.

And as with most threats to democracy, the best defense is a more informed voter. If you're an American, you're most likely a partisan or have partisan leanings; you're more likely to respond positively to news that helps your candidate or harms their opponent, even when it involves foreign tampering. Resist that impulse. It's appropriate only within the realm of partisan politics; it's inappropriate and dangerous when we're talking about attacks that transcend the political realm.

Part of this can be laid at the feet of the media that drives much of our political discussion. The national security threat of a known hack of State Department networks is orders of magnitude larger than that of a hack on the Secretary of State's email server. A political debate driven by national security policy would give far more weight to the former. A political debate driven by scandal favors the latter.

This problem is driven by the fact that news organizations respond to the appetites of their audiences; the quality of political media is often no better than the quality of those appetites. It's one thing for us to consume editorial and opinion pieces that agree with our political views; when we decide to filter reporting of national events with the same prejudices, we make it impossible to hold a rational debate with people who disagree with us.

My personal strategy is to deliberately expand my media diet with plenty of international sources, especially the BBC. Perhaps these sources have political bias when covering their own countries, but they're unlikely to fall prey to American political influences. I avoid partisan news outlets on both sides not because I disagree with them, but because I find them non-credible sources, both for what they select as newsworthy and their actual coverage. I sometimes listen to Rachel Maddow, but that's part of my entertainment diet in addition to my regular news diet, not in lieu of it.

Likewise, resist attempts by the media and political organizations to normalize hacked documents by citing them as unbiased sources. The National Republican Congressional Committee cited hacked documents from the DNC in a campaign ad in Florida; political newspaper The Hill ran with a story about DNC manipulation of primary races in Pennsylvania. (The Hill at least points out that the intentions of the leaker are "interesting" but then drops the topic for the rest of the story.) Both actions presume that using the documents in question is legitimate; both also inherently assert that the documents are true and accurate. The former is up for debate; the latter is entirely uncertain. Hacks are done for a reason, public releases are done for a reason, and electronic documents can be modified easily; all of these should contribute to a healthy dose of skepticism when you're evaluating such news. (This is not to suggest that the leaked DNC documents were falsified; the resignations of three DNC officials thereafter implies they were basically sound. However, if I were going to design a disinformation campaign, I'd start with true documents and then follow up with false ones.)

If you're involved in politics, it's time to up your information security game; if you're not involved but have technological chops, now is an excellent opportunity to make your skills known to community organizations who might need you. It's too late this election cycle to walk into a campaign and volunteer to see their most valuable data, but anyone who gets involved in 2016 becomes a known resource in 2018 and later.

This is a nonpartisan prescription: we know that Democrat organizations have been targeted, but there's no reason to think that Republican groups have better security. I can think of a dozen reasons why foreign governments would be just as interested in Republican data, so until further information is available, I'm assuming that it's more accurate to say the Republicans "are not known to be hacked" than "were not hacked."

As Jefferson (supposedly) said, vigilance is the price of liberty. He didn't have computer networks in mind, but this is one of those times when it's even more important than usual.

by Josh Centers

W1-powered AirPods Usher in a New Era of Wireless Audio

Like it or not, Apple is moving away from the nigh-universal headphone jack, at least on the iPhone line. The just-announced iPhone 7 and 7 Plus, as expected, lack an analog 3.5mm headphone plug (see "iPhone 7 and 7 Plus Say "Hit the Road, Jack."," 7 Sept 2016). But the good news is that Apple understands that existing wireless audio solutions are lacking; Bluetooth sound quality is mediocre, and more importantly, it's difficult to use Bluetooth headphones with multiple devices. AirPlay switches easily between devices, but its dependency on Wi-Fi means that the power draw is too high for mobile devices.

To counter those problems, Apple has introduced the new W1 chip, which will power the company's upcoming flagship AirPod wireless headphones, as well as new Beats headphones. The $159 AirPods are expected in late October 2016. Apple is also incorporating the W1 chip into its new $299.95 Beats Solo3 Wireless headphones, plus the forthcoming $199.95 Powerbeats3 Wireless workout earphones, and the $149.95 Beatsx earphones.

The proprietary W1 chip brings several advantages: up to 5 hours of battery life, support for various sensors, purportedly superior audio quality, and most important, easy connections. You'll be able to pair a W1 device merely by placing it close to an iOS device. Once connected, settings are synced to an Apple Watch, if you have one, and over iCloud to any of your other Apple devices (although Apple didn't mention the Apple TV). You can simultaneously connect to your iOS devices, Macs, and Apple Watches and, according to Apple, switch seamlessly between them.

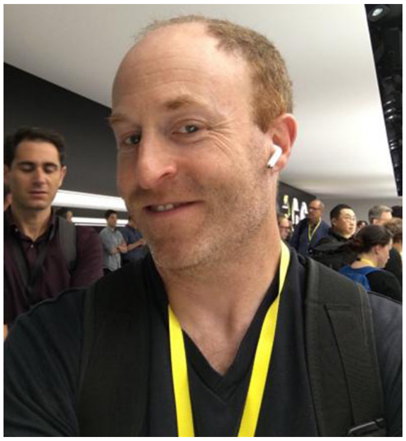
The W1's technology is based on Bluetooth, so you can use W1 headphones with unsupported devices, but you will have to pair them just as you would any other Bluetooth device.

Apple's AirPods are the flagship W1 device. They have a futuristic look, reminiscent of the omnipresent headsets featured in the movie "Her," and are similar to the existing EarPods, with elongated microphone stems that extend from your ears.

Like the EarPods, AirPods include a microphone — two microphones, actually. To activate Siri, double-tap either AirPod. Special sensors detect where your voice is coming from and focus the microphones appropriately. The AirPods also include optical sensors that detect when the AirPods enter or exit your ears — the AirPods pause audio when you remove them and you can configure them to play audio when you insert them. You can even use just one AirPod at a time if you wish, which is a good idea at times for safety reasons.

Because they're so small and have so little room for batteries, a fully charged AirPod runs for only 5 hours, but Apple has a few special tricks to improve the situation. The AirPods come with a special charging case that can provide a 3-hour charge in just 15 minutes. Apple provided few details about the case but claims it extends AirPod battery life up to 24 hours. You charge the case itself via a Lightning connector.

TidBITS Security Editor Rich Mogull was on site at the Apple announcement and had a chance to try the new AirPods. He verified that they fit similarly to EarPods, so if you dislike that fit, don't waste your money on the AirPods. However, Rich said that they're overall more comfortable, because there's no cable drag. Even so, he wasn't sure that he would use them for running.



The AirPods and the W1 chip offer legitimate advantages over existing wireless technologies, but be aware of the additional platform lock-in, since these devices will require compatible Apple hardware for full functionality.

by Tim Sullivan

Rumors and Reality

Links and copyright rules: the Court of Justice of the European Union has decided that a website that merely links to material that infringes copyright can itself be found guilty of copyright infringement, provided only that the operator knew or could reasonably have known that the material was infringing. Worse, they will be presumed to know of this if the links are provided for "the pursuit of financial gain".

Gotcha 1: "financial gain" includes any site the runs ads.

Gotcha 2: the links can drill down through several web sites. If a link directs the reader to a site which in turn has links to a site which contains copyrighted material then the first site is guilty of infringement.

Gotcha 3: pointing out and linking to a site that has plagiarized material is a no-no.

It makes my head spin.

Note to self from abroad: If you're too cheap to get a SIM card that will work overseas in your phone or a portable wi-fi, there's not much point in downloading those apps that translate the local writing or spoken language into something I can understand.

One converter and a two-outlet extension cord just does not cut it when you are trying to charge a laptop, an iPad, two iPhones, a portable wi-fi unit, and a fitbit.

The Find My Car app can be thought of as a Find My Hotel app. Once you get the hang of how to use it, it's really handy for finding your way back to your hotel in a strange city.

For those who have concerns about their privacy, I recommend an article in November Consumer Reports: "66 Ways to Protect Your Privacy Right Now." The auther describes her own steps to minimize her digital life being passed around. Then she list specific steps that you can take. She offers a handful of links that could be very useful. My favorites are haveibeenpwned.com and 10minutemail.com.

Pwned is a term applied to game opponents when they have been soundly defeated; in this context it applies to companies and their customers that have been hacked and their data stolen.

The second site will provide a temporary email address to be used in those sites that require such things. There are many times I want to check out a site for free stuff even though I know it will generate a lot of unwanted emails down the line. I'll be made up email addresses from now on.

Software Review

Apple Updates

Pro Video Formats 2.0.5
Post Date: Oct 27, 2016 – 7 MB

System Requirements
– OS X 10.11 or later

What's New in Pro Video Formats 2.0.5
- ProRes wrapped in MXF OP1a file container
- Support for AVC-Intra LT
- Support for playback of MXF wrapped files in QuickTime Player X on macOS Sierra

Pro Video Formats includes support for the following professional video codecs:

- Apple Intermediate Codec
- Apple ProRes
- AVC-Intra
- AVC-LongG
- XAVC
- XF-AVC
- DVCPRO HD
- HDV
- XDCAM EX / HD / HD422
- MPEG IMX
- Uncompressed 4:2:2

Pro Video Formats also includes the following MXF support:

- Native import, edit, and share of MXF files with Final Cut Pro X and Motion
- MXF share presets for Compressor
- MXF OP1a export

macOS Sierra 10.12.1 Update
Oct 27, 2016 – 1.36 GB

System Requirements
– macOS Sierra 10.12

The macOS Sierra 10.12.1 update improves the stability, compatibility, and security of your Mac, and is recommended for all users.

This update:

- Adds an automatic smart album in Photos for Depth Effect images taken on iPhone 7 Plus
- Improves the compatibility of Microsoft Office when using iCloud Desktop and Documents
- Fixes an issue that may prevent Mail from updating when using a Microsoft Exchange account
- Fixes an issue that caused text to sometimes paste incorrectly when using Universal Clipboard
- Improves reliability of Auto Unlock with Apple Watch
- Improves security and stability in Safari

iTunes 12.5.2
Oct 27, 2016

System Requirements
– 400MB of available disk space

This update includes stability and performance improvements. It also:

- Fixes an issue where albums may play in an unexpected order
- Resolves a problem that prevented lyrics from appearing while listening to Beats 1

iOS 10.1 Information

This update includes Portrait Camera for iPhone 7 Plus (beta), transit directions for Japan, stability improvements and bug fixes.

Camera and Photos

- Introduces Portrait Camera for iPhone 7 Plus that creates a depth effect that keeps your subject sharp while creating a beautifully blurred background (beta)

- People names in the Photos app are saved in iCloud backups

- Improved the display of wide color gamut photos in the grid views of the Photos app

- Fixes an issue where opening the Camera app would show a blurred or flashing screen for some users

- Fixes an issue that caused Photos to quit for some users when turning on iCloud Photo Library

Maps

- Transit support for every major train, subway, ferry, and national bus line, as well as local bus systems for Tokyo, Osaka, and Nagoya

- Sign-based transit navigation including layouts of all underground structures and walkways that connect large transit stations

- Transit fare comparison when viewing alternative transit routes

Messages

- New option to replay bubble and full screen effects

- Messages effects can play with Reduce Motion enabled

- Fixes an issue that could lead to contact names appearing incorrectly in Messages

- Addresses an issue where Messages could open to a white screen

- Addresses an issue that could prevent the report junk option from displaying with unknown senders

- Fixes an issue where videos captured and sent in the Messages app could be missing audio

Apple Watch

- Adds distance and average pace to workout summaries in the Activity app for outdoor wheelchair run pace and outdoor wheelchair walk pace

- Fixes issues that may have prevented Music playlists from syncing to Apple Watch

- Addresses an issue that was preventing invitations and data to appear in Activity Sharing

- Fixes an issue that was allowing Activity Sharing to update over cellular when manually disabled

- Resolves an issue that was causing some third-party apps to crash when inputting text

Other improvements and fixes

- Improves Bluetooth connectivity with 3rd party accessories

- Improves AirPlay Mirroring performance when waking a device from sleep

- Fixes an issue where playback would not work for iTunes purchased content when the “Show iTunes Purchases” setting is turned off

- Fixes an issue where certain selfie apps and face filters used with the FaceTime HD Camera on iPhone 7 and iPhone 7 Plus did not display a live preview

- Fixes an issue in Health where individual strokes are converted to separate characters when using the Chinese handwriting keyboard

- Improves performance of sharing websites from Safari to Messages

- Fixes an issue in Safari that caused web previews in tab view to not display correctly

- Fixes an issue that caused certain Mail messages to be reformatted with very small text

- Fixes an issue that caused some HTML email to be formatted incorrectly

- Fixes an issue that in some cases caused the search field to disappear in Mail

- Fixes an issue that could prevent Today View Widgets from updating when launched

- Fixes an issue where Weather widget sometimes failed to load data

- Fixes an issue on iPhone 7 where Home Button click settings would not appear in search results

- Fixes an issue that prevented spam alert extensions from blocking calls

- Resolves an issue that could prevent alarm sounds from going off

- Fixes an issue where audio playback via Bluetooth would cause the Taptic engine to stop providing feedback for some users

- Resolves an issue preventing some users from restoring from iCloud Backup10

Security Update 2016-006 (10.10.5)
Oct 24, 2016 – 473.6 MB

System Requirements
- OS X Yosemite 10.10.5

Security Update 2016-006 is recommended for all users and improves the security of OS X.

Security Update 2016-002 (10.11.6)
Oct 24, 2016 – 414.9 MB

System Requirements
- OS X El Capitan 10.11.6

Security Update 2016-002 is recommended for all users and improves the security of OS X.

watchOS 3.1 Information

This update includes improvements and bug fixes.

- New option to replay bubble and full screen effects in Messages
- Messages effects can play with Reduce Motion enabled
- Fixes an issue that could cause the notification for Timer complete to be delivered twice
- Resolves an issue that could prevent Apple Watch Series 2 from fully charging
- Resolves an issue where Activity rings may disappear from the watch face
- Fixes an issue that prevented Force Touch options from appearing in some third-party apps

Brother Printer Drivers 4.1 for OS X
Oct 6, 2016 – 243.6 MB

System Requirements
- OS X Mountain Lion 10.8
- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12

This update installs the latest Brother printing or scanner

Share Keystone MacCentral with other MACaholics

Name ____

Address ____

City ____ State ___ Zip ____________

Home Phone __________________________ Day Phone __________________________

E-mail Address ____

Date _________________ Is this ❍ Renewal or ❍ New?

How did you hear about us? ____

Dues for one person are ❍ $20/yr. Family or Corporate dues are ❍ $30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

Keystone MacCentral
Membership Chair
310 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral meetings are held at 6:30 p.m. on the 3rd Tuesday of the month at Bethany Village Retirement Center, 5225 Wilson Lane, Mechanicsburg, PA 17055