January 2019
Vol. XXX, No 1

KEYSTONE MacCentral

printout

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

January Program

During our program this month we will show a condensed version of a recent iPad and Mac presentation. After that we will view some short videos regarding the new Mac Mini and a quick video from iFixit showing what can be upgraded on the new MacBook Air.

The latest scam/extortion on the Internet is the ominous letter that implies that a hacker now controls your identity and is going to destroy your life. We'll have a short demo of a common encryption standard and how easy we can crack it online with free tools. Then we'll view a short video about password hacks and some good advice on how to create good password. After this we will open up a roundtable discussion by our members about their experience with Password Managers.

Meet us at

Bethany Village Retirement Center

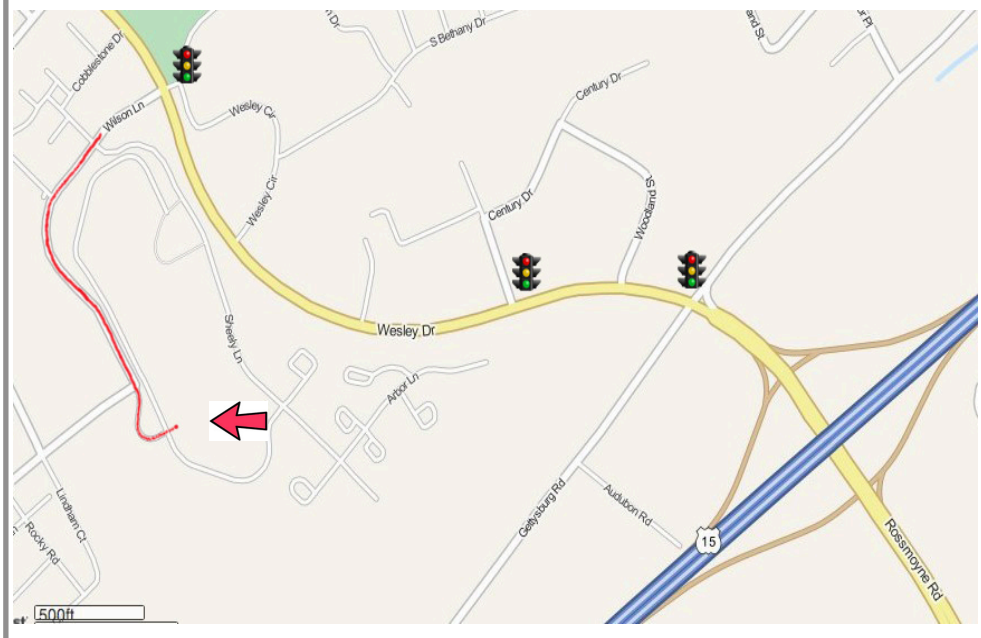
Education Room

5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, January 15th 2018 6:30 p.m.

Attendance is free and open to all interested persons.

Contents



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 Adam Engst

"Hacked Account" Blackmail Spam on the Rise — Beware!

Note: Not sure if it is coincidence or if the hacker was monitoring my source, but I received essentially the same threat a few weeks later. He/she/it was unable to find any "joys" on my computer though.

Editor

You open your inbox and see a message labeled "Change your password immediately. Your account has been hacked." Inside, the email contains what it claims is one of your passwords, a threat, and a demand for money. The password is indeed one you've used in the past — how did the hacker get it? Could you really have been infected with malware?

This "blackmail spam" has been inundating inboxes across the Internet, and while there's no way to know how effective it is, it has caused plenty of raised pulses. Written in deliciously fractured English, the email message purports to be from a hacker who has taken over your computer and installed spyware that has revealed your brazen browsing habits. The hacker also claims to have taken pictures of you (staring intently, one presumes) while you click through "the big delight of your favorite resources" and threatens to share them with your contacts and brick your computer unless you send a payment using Bitcoin.

What has caused concern for lots of people is that the blackmail spam "proves" that it's legitimate by showing you a password that you've used in the past. (This is often the case, but not universally so. Most copies of this spam that I've received include passwords I never used.) Hopefully, the revealed password is not one that you're still using, since it was extracted from one of the many large password breaches that have occurred over the last decade. To see which breaches might include one of your passwords, check your address at Have I Been Pwned. (It's worth noting that most of the passwords that attackers have decrypted are short and insecure. If your password was over 12 characters and didn't use dictionary words or well-known patterns, it may have resisted decryption.)

I greet you!

I have bad news for you.

27/08/2018 - on this day I hacked your operating system and got full access to your account.

On that day your account password was: b8a7d0

It is useless to change the password, my malware intercepts it every time.

How it was:

In the software to the router to which you were connected that day, there was a vulnerability.

I first hacked this router and placed my malicious code on it.

When you enter to the Internet, my Trojan was installed on the operating system of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts}.

A month ago, I wanted to lock your device and ask for a small amount of money to unlock.

But I looked at the sites that you regularly visit, and came to the big delight of your favorite resources.

I'm talking about sites for adults.

I want to say - you are a big pervert. You have unbridled fantasy!

After that, an idea came to my mind.

I made a screen shot of the intimate website where you have fun (you know what it is about, right?).

After that, I took off all your joys (using the camera of your device). It turned out beautifully, do not hesitate.

I am strongly believe that you would not like to show these pictures to your relatives, friends or colleagues. I think $915 is a very small amount for my silence.

Besides, I spent a lot of time on you.

I accept money only in Bitcoins.

My BTC wallet: 1LwibrnKAKu4kt4svRLYdUP3aW7:3Y78zl.

You do not know how to replenish a Bitcoin wallet?

In any search engine write "how to send money to a BTC wallet".

It's easier than send money to a credit card!

For payment you have a little more than two days (exactly 50 hours).

Do not worry, the timer will start at the moment when you open this letter. Yes, yes... it has already started!

After payment, my virus and dirty photos with you self-destruct automatically.

Narrative, if I do not receive the specified amount from you, then your device will be blocked and all your contacts will receive a photo with your "joys".

I want you to be prudent.

- Do not try to find and destroy my virus. (All your data is already uploaded to a remote server.)

- Do not try to contact me (this is not feasible I sent you an email from your account.)

- Various security services will not help you: formatting a disk or destroying a device will not help either since your data is already on a remote server.

P.S. I guarantee you that I will not disturb you again after payment, as you are not my single victim. This is a hacker code of honor.

From now on, I advise you to use good antiviruses and update them regularly (several times a day)!

Don't be mad at me, everyone has their own work.

Farewell

To make this painfully clear, everything in the message other than your email address and breached password is fabricated. Your computer has not been hacked, there is no malware spying on your browsing, no pictures of you have been uploaded to a remote server, and so on. You have nothing to worry about, and you should feel free to mark the message as spam and get on with your life.

If your friends and colleagues ask you about similar blackmail spam, point them to this article and reassure them that they have nothing to worry about. Unless, of course, they're still using the password that was revealed, in which case they should change it immediately.

Nonetheless, this spam marks what I fear is a turning point in malicious Internet communications. Most spam and phishing messages are almost entirely generic, with their main customization being your email address and occasionally your name. Sometimes they spoof a friend's address or are even sent from a friend's compromised account, but that's about it. Such spam messages are convincing — to the extent that they are — only because of some larger context or because they tap into common desires to get or save money, be more attractive, or partake of some of that brazen browsing. (I'm trying hard to avoid triggering overeager spam filters with more specific words here!)

But not this message. The believability of this blackmail hinges on the fact that — in theory — only you know your password. If the blackmailer can know your password, you think, perhaps their other claims are true too. They're not, but even people whose browsing habits are always G-rated often report a moment of panic. I presume those who still use ancient insecure passwords experience more than a moment of panic, and well they should.

The problem is that old stolen passwords are just the tip of the iceberg when it comes to information about us that's readily available online. This blackmail spam combines only two bits of information — your email address and password. What happens when similar attacks expand the amount of information they use?

Some breaches, like the Apollo breach that took place in July 2018, include lots of other types of personal data — places of employment, roles held, locations, and corporate revenue numbers. Even more data is available in public databases. The New York Times recently published an article about apps that use voter registration and voting records to encourage friends to vote, but it's easy to imagine that data being used for malicious purposes. Then there are real estate records, bankruptcy filings, divorces, and so on.

APOLLO In July 2018, sales engagement start up Apollo left the database contain billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive informations such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organization.

Blackmail spam taken to its logical extreme is the ultimate example of why we all have something to hide. It's not that anyone has necessarily done anything that embarrassing, but the chance that we could be blackmailed into paying to keep certain facts under wraps is increasing. Imagine blackmail spam that threatens to reveal your likely voting history to everyone in your neighborhood who is registered with the other party. Or blackmail spam that says it will tell everyone on the Internet with your last name about your bankruptcy or divorce. Blackmail spam doesn't even have to be true to be damaging. What would be the hit to your career if a spammer targeted everyone at your company's domain name with an anonymous message that accused you of having committed sexual assault a few years ago and said that the sender was too terrified to identify themselves?

I don't like to feed privacy paranoia, but as criminal organizations acquire more data science skills and ever larger datasets, such attacks will become all the more sophisticated and believable. It may not happen overnight — people with such skills can usually find legitimate employment more easily—but just as organized crime groups now have or can hire skilled programmers to create malware, they'll eventually be able to find people who can combine every available piece of data about you and weaponize it in numerous ways. Similarly, it has become clear that governments aren't above sowing fear, dissension, and

confusion in the general populace, and they probably have the resources to do this already.

The worst part is that I can't imagine a good defense against such attacks. Spam filters work against traditional spam because you're protected if you don't see the message. But you not being aware of a threat won't prevent a blackmailer from carrying it out. Blocking payment methods or tracking payments may be effective in the real world, but cryptocurrency systems make such payments harder to track, if not completely anonymous when the money comes out of an exchange. But even that wouldn't protect against a dedicated state actor looking to introduce strife into society.

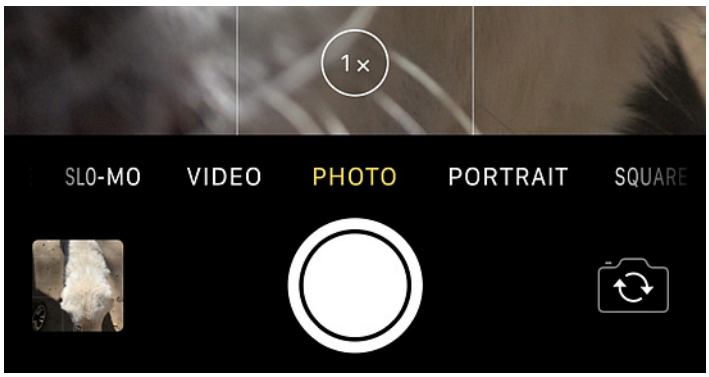
Enhanced privacy legislation that limits the amount of data available about us online could help prevent or reduce the severity of these attacks. Though it's far from perfect, Europe's GDPR is a step in that direction. Here in the United States, however, serious privacy legislation probably won't stand a chance—at least until the politicians who oppose it have had their lives laid bare for all to see, just like the rest of us.

by Josh Centers

Using the iPhone Camera's Zoom Button

In all iPhones, when you're taking a photo with the Camera app, you can zoom by putting two fingers on the viewfinder and moving them apart — the traditional pinch-to-zoom. However, the zoom level can be hard to control precisely, which becomes an issue on the "big" iPhones — the iPhone 7 Plus, iPhone 8 Plus, iPhone X, iPhone XS, and the iPhone XS Max. That's because those models sport dual cameras that support 2x optical zoom — at any level other than 1.0 or 2.0 you're using digital zoom that trades zoom level for picture quality. (As Glenn Fleishman notes at Macworld, the iPhone might use digital zoom regardless of zoom level, depending on the conditions).

To address that, Apple enhanced the Camera app on those models with an additional way of zooming, a visible zoom button in the viewfinder, above the shutter button.



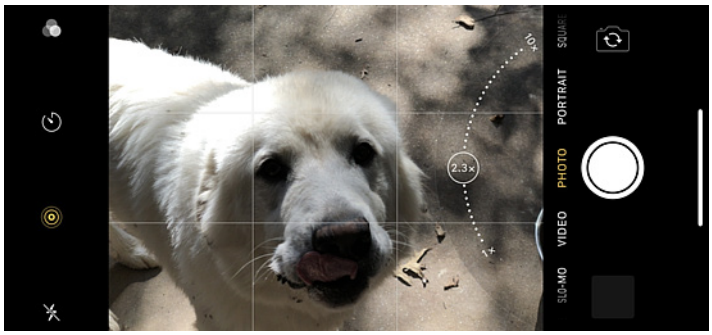
We've recently learned that not everyone realizes what this zoom button can do. It has three functions:

1x/2x zoom toggle: Tap the button to switch between 1x and 2x. If you're on an oddball zoom level, like 7.4x, a quick tap takes you back to 1x.

Incremental zoom control: Place a finger on the button and drag to move the circular slider between 1x and 10x zoom, in increments of 0.1. The button doesn't move when you switch orientations, so in landscape orientation, dragging it down increases the zoom and dragging it up reduces it. In portrait orientation, dragging it to the left increases zoom and dragging it to the right reduces it.

Zoom level indicator: When you use the traditional pinch-to-zoom approach, the zoom button shows the zoom level.

If you want to see the zoom button in action, here's a quick video showing how to use it.



by Jeff Carlson

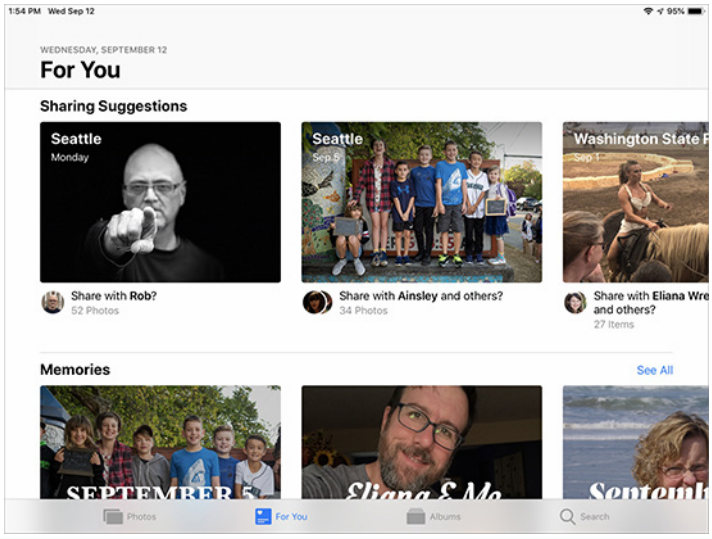
Inside iOS 12: Photos Encourages More Engagement

The iPhone has become the primary camera for many people because it's so convenient and it takes high-quality photos. But an often overlooked factor in its popularity is the social aspect: you can share photos immediately to Instagram or Facebook, or directly with friends and family members, without first having to offload them to a computer.

Apple's improvements to the Photos app in iOS 12 focus on the social side of modern photography, encouraging you to revisit, discover, and share images from your library. There are also a few importing and editing changes worth mentioning.

Photos For You (Yes You)

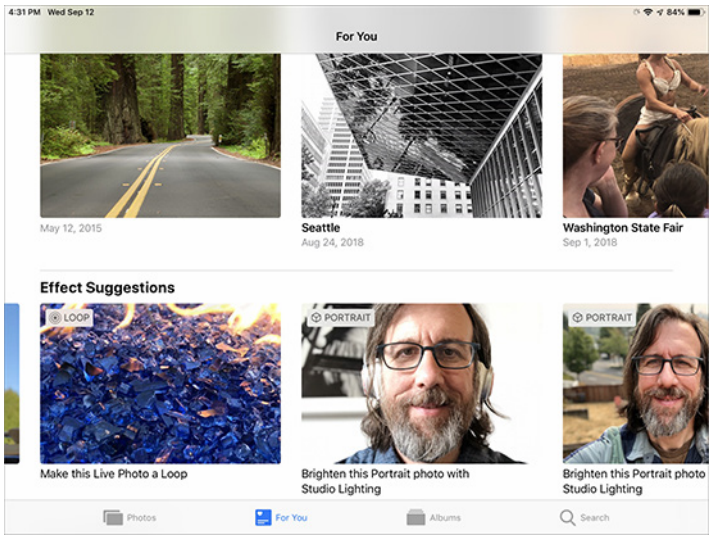
Apple has leveraged its For You feature in iTunes successfully — even though I see a lot of repetition, I still turn to it often to see what music it suggests. In iOS 12, the Photos app's new For You screen incorporates more than just Memories, the button it replaces on the toolbar.



Memories — those collections of photos and videos turned into an automatically generated movie — share space in For You with the following additions, which may show up in various orders:

Featured Photos: Photos mostly pulls these images from the pool of photos you've marked as Favorites, although some recently edited shots that aren't favorited also pop up in my feed. The idea seems to be to expose you to images you liked, perhaps to bring a smile to your face or encourage you to share them. A dozen images appear in this category every day; there's no mechanism to change or display others other than waiting to see what shows up the next day.

Effect Suggestions: This category takes advantage of the lighting effects in Portrait Mode photos and animation options in Live Photos (such as looping, bouncing, or smoothing the video), suggesting that you might try applying those effects for the displayed images. When you view one of the suggestions, you can jump to the photo in your library, or tap Apply to Original to add the effect without going through the editing interface. So far I've seen only those two types of effects, but in theory, Photos could suggest applying filters or other edits as well. Curiously, even after you apply an effect, the image stays in the Effect Suggestions row until the next day, (with an option to revert the edit if you change your mind).



Shared Album Activity: The Shared category used to have its own button at the bottom of the Photos screen, but now Apple groups it in with Albums. But since For You is all about staying on top of what has happened recently, the new Shared Album Activity category reveals photos you or members of group shared albums in iCloud Photo Library have contributed recently, as well as likes or comments on those photos.

Sharing Suggestions and Recently Shared: Photos that include contacts you've identified using the People feature can show up in these two categories. More on new sharing features shortly.

It's worth pointing out that the items in the For You screen are identical on my iPhone X and iPad Pro. Earlier versions of Photos could bring up different Memories suggestions,

and facial recognition was done independently on each device. Now they're synced through iCloud. Alas, the Photos apps in macOS 10.14 Mojave and tvOS 12 lack these For You features.

Albums

Apple shuffled the Albums screen a bit, putting My Albums and Shared Albums up top, followed by People & Places. Photos in iOS 12 more prominently lists the Media Types — videos, selfies, Portrait mode shots, and the like. A new Animated type includes Live Photos to which you've applied effects, along with any animated GIFs that you've saved to your library.

Under the Other Albums category, the app breaks out the Imports, Hidden, and Recently Deleted albums.

Sharing Suggestions and Pooling Photos

Sharing photos goes beyond just texting a selfie to a friend or posting a snapshot on social media. Have you attended an event with friends or family and wished you could see everyone else's photos? (Apart from everyone posting them to long Facebook comment chains, that is.)

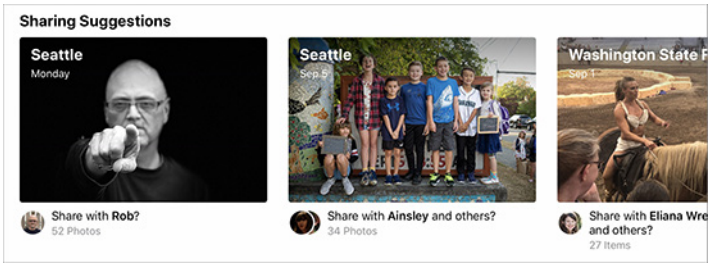
Apple has offered iCloud Shared Albums for a while, but those are more permanent and structured, requiring that you set up the album and invite people to subscribe to it. If you create several one-off shared albums, they start to clutter up the list.

Photos in iOS 12 introduces the option to share photos by sending someone a link, versus sending image files outright, but it may not work the way you expect.

You have several paths to get to this feature. The easiest is to select one or more photos, tap the Share button, and tap Copy iCloud Link. Photos generates a URL and copies it to the clipboard, after which you can paste it into any text field, such as an email message or text. Following that link takes the recipient to a Web page containing thumbnails and the option to download or add the images to their iCloud Photo Library.

The more clever version of this feature is called Sharing Suggestions, and it's triggered when people you know — more specifically, folks you've identified in the People feature — appear in your photos. The app also looks at the location data embedded in the images to guess events. For example, when my family and I went to the state fair a couple of weeks ago, Photos listed the location as "Washington State Fair," not the city of Puyallup where it's located.

When these two criteria intersect, you may see prompts to share the images under Sharing Suggestions on the For You screen. Or, in the Photos screen, you can tap the > button to the right of the date or location heading, tap the More button (•••), and choose Share Photos. If an identified person appears in any of the photos, you're asked if you want to share with them; otherwise Photos asks if you want to share "with friends."



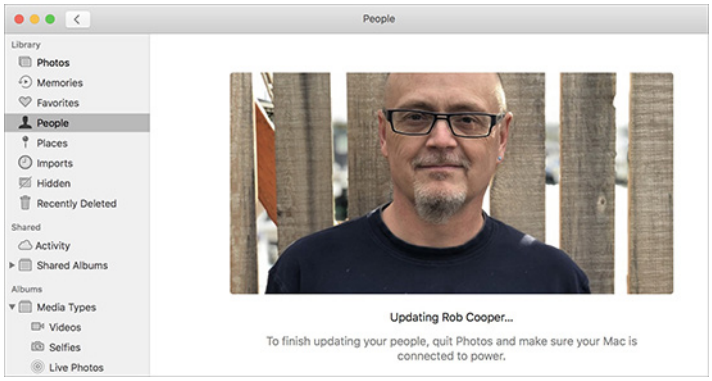
Time for a Rant: Why Does Photos Have to Be Such a Black Box?

Before I get into the mechanics of how this works, I need to rant briefly about the opaque inner workings of the Photos app.

To test the Sharing Suggestions feature, I invited a friend who was also running iOS 12 on his iPhone to go photograph a spot in the Fremont neighborhood of Seattle. Then we'd share the shots we captured, making sure we each took pictures of the other so facial recognition could kick in.

First lesson: don't expect quick results. In the 10 or 15 minutes it took for us to walk to a nearby coffee shop, get drinks, and set up at a table, Photos didn't recognize that there was a person in my images. Perhaps I was expecting too much, too soon; Photos puts off computationally expensive tasks like facial recognition until the device is plugged into power, so as not to drain the iPhone's battery in the background. I understand that.

However, there's no way in iOS to scan and identify a person manually, even just for one image. My friend Rob didn't appear in the People album, even though other photos that include him exist in my library. If he had appeared, I could have tapped his name and hoped that Photos would find the new photos as possible matches.



In fact, Photos in iOS and on the Mac (in this case, in 10.13 High Sierra) only wants to deal with people on its own schedule, when the device is connected to power, and preferably overnight. The Mac version of Photos is even more frustrating, telling me, "To finish updating your people, quit Photos, and make sure your Mac is connected to power."

This is yet another example of one of my biggest gripes with the Photos app. It's so intent on doing everything for you that it provides no way to intervene and force it to do something specific. How many times have I wanted Photos to sync with iCloud Photo Library so new images appear on my iPhone, iPad, and Mac? More than I can count. It doesn't matter whether I'm using a cellular Internet connection, a janky coffee shop Wi-Fi network connection, or my relatively speedy home router. Photos sometimes syncs right away, and other times delays syncing until it feels like it. Impatient users can go pound sand.

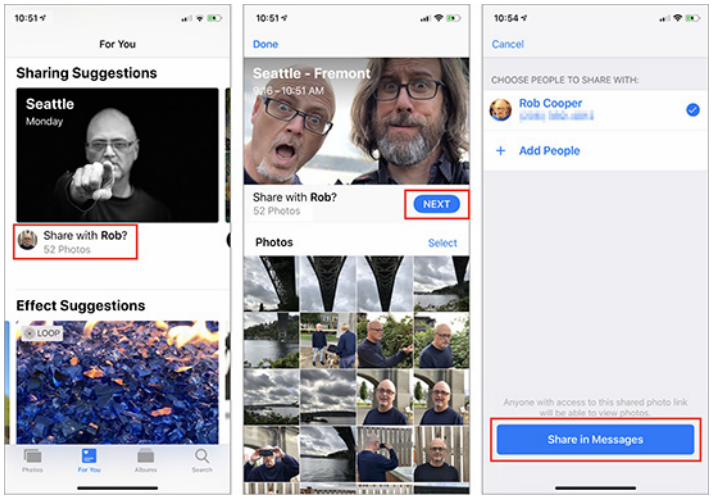
In this case, I thought I could perhaps cheat the process and identify Rob in Photos on my Mac, since a mechanism exists for manually doing that (choose Window > Info with an image selected, and click the Add Faces button). The images themselves had synced, so I identified Rob in two of the images—maybe that would prime the pump?

No. Even with the Photos apps running on the iPhone and my MacBook Pro, and the iPhone plugged into a portable battery charger to eliminate battery life savings as a holdup, it took Photos more than an hour at the coffee shop before the app recognized Rob as a person. Oddly, it did so based on other photos in which Rob appeared in my library, and he didn't show up in the People album until much later.

In short, don't expect to pool your photos with your friends right after an event ends. This is an instance when the 3D Touch feature would come in handy: press on a face to bring up a circle to define where a person's face is, and assign an identity. I know it's Rob in my photo, and I should be able to tell Photos that, instead of waiting for the app to get around to asking.

Meanwhile, Back at Sharing Suggestions

With that rant out of the way, the Sharing Suggestions feature is actually pretty neat. In the For You screen, if a collection of photos includes a person and a similar timestamp and location, Photos assumes you were with that person and asks if you want to share your images with them. You can also view the option in the Photos screen by tapping the (>) button to the right of a date or location heading, tapping the blue More (•••) button, and choosing Share Photos. You can share with anyone, not just the people identified in the photos.



Instead of sending image files, Photos generates an iCloud link and sends it using Messages. If the recipient is also running iOS 12, they can add your pictures — at full resolution — to their Photos library; if not, they have the option of downloading the files. When someone uses the latter option, Photos converts the HEIC originals to JPEG files.

Furthermore, if you appear in their photos, Photos asks them if they want to share their images back to you using the same Messages mechanism. Everyone involved in the conversation ends up with all of the photos from the get-together that they choose to add or download.

Note that these shared groups are active for only one month, after which the link expires, so don't put off snagging shared photos that you want to keep.

As I said, this new sharing approach is a neat idea, but there are some problems:

- Most annoying, even beyond the lag in identifying people mentioned above, is that there's no attribution for who took each photo in the pool. By blending my shots with Rob's, we ended up with a collection of photos where many of them could have been taken by him or me, and I don't know which is which. It's just as important to include authorship as it is to be able to combine shots. I'm amazed Apple didn't include some owner metadata and a tag denoting it.

- The iCloud link that's generated applies only to the state of the photos at that time. When I edited some images (such as converting a few to black and white), those changes weren't reflected on Rob's iPhone. In other words, this is not an active pool of photos on an Apple server somewhere; Messages provides only the conveyance. If I click the original link that was created, in fact, none of the edits appear there either.

- The Photos app doesn't know that I've already shared those images with Rob. The following day, they appeared once again as a Sharing Suggestion, asking me if I wanted to share them with Rob.

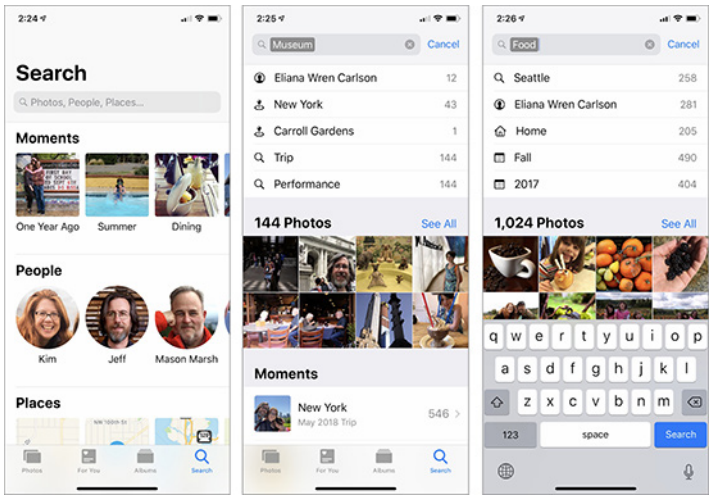
Speaking of Messages, in iOS 12, you now share image files from your Photos library using a new Photos mini-app available under the text field. Previously, you'd tap the camera button to either take a snapshot with the camera or browse recent photos.

Search Suggestions

I've written several editions of Take Control of Your Digital Photos, which, at its core, is all about finding the photos we've put so much time and effort into capturing and storing. If we're just stuffing images into a virtual shoebox, then what's the point in using anything beyond Finder folders?

To that end, Apple has expanded the search capabilities in Photos for iOS. Search is now a prominent category button in the toolbar, and tapping it displays suggestions for

Moments, People, Places, and Categories. The Moments and Categories options are all generated using machine learning, resulting in options such as (in my case) Summer, Dining, Sporting Events, Museum Visits, Trips, and the like. Tapping Museum Visits, for example, displays more specific options, such as names, keywords, and locations. A new Groups row reveals photos where two or more named people appear together in the same photo.



Photos' search is quick to display related photos and other metadata, which you can tap to refine the search. Apple says you can "combine keywords in searches… for even better results," though this seems to be limited to choosing multiple suggested terms. Typing "California sunset" netted me nothing, but searching for "California," tapping the first result, and then typing "sunset" did work.

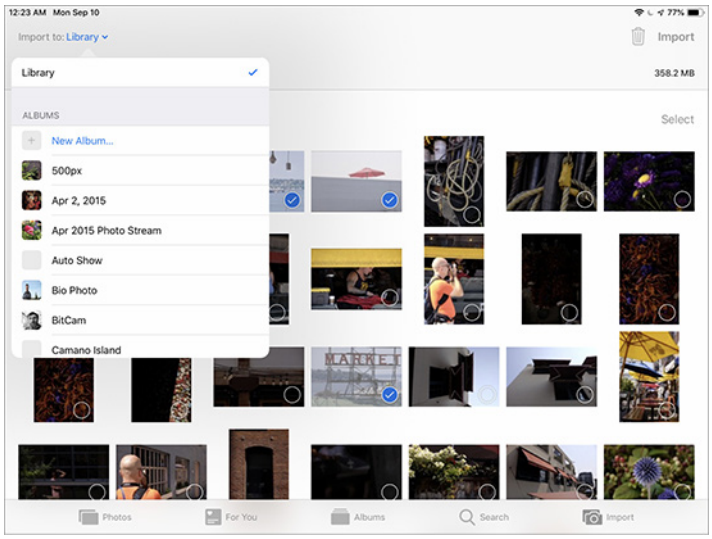
Unfortunately, Photos still ignores some basic metadata included in every image file, such as camera model; if I type "Fuji" in the Search field to reveal all the photos taken with my Fujifilm X-T1, Photos comes up empty.

Import(ant) Improvements

For people who import photos from traditional digital cameras into an iPad or iPhone, this release of Photos will be a relief.

When you connect a memory card using Apple's Lightning to SD Card Reader, Photos displays thumbnail previews in the Import screen much faster than in the past. I had pretty much stopped doing large imports to my iPad Pro because of the painful pace of just drawing those images.

You can also now specify a destination album for the images, and see how many images are selected for import, how many are on the card, and how much storage space they occupy.



Editing Raw Images

Lastly, Apple says you can edit raw images on iPhone or iPad models with an A9 chip or later, although this claim has generated some confusion because raw support in iOS isn't new.

Quick background: iOS has included native raw image support at the operating system level since iOS 10 appeared in 2016. Before that, if you imported a raw file directly onto an iPad or iPhone, editing it would affect only the small JPEG preview your camera creates to display a preview on its LCD.

Editing raw images in iOS 10 and later produced better results due to that raw support, but there was a twist. The Photos app in iOS 10 and iOS 11 doesn't edit the raw image directly. Instead, the app generates a high-quality JPEG from the raw data and edits that copy.

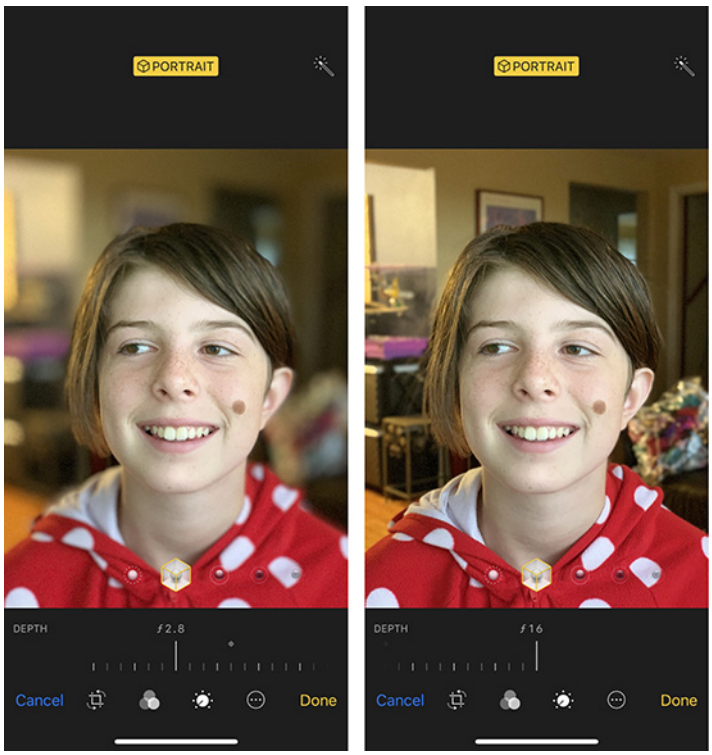
In the Photos interface, it looks like you're working with just a single image. And, because the edits are non-destructive, adjustment data is stored separately, such as noting that exposure is at 0.13. When Photos syncs the raw image to the Mac, the same settings apply to the actual raw image, since Photos in macOS does edit raw files directly. (See "How Raw Works on iOS," by Nik Bhatt, formerly a lead on Apple's Aperture and iPhoto teams and now the creator of the utility RAW Power.)

Back to iOS 12: Since the A9, A10, and A11 processors are much more powerful than the generations before them, the Photos app can now work directly with the raw files. If my experience using an iPhone X and a 9.7-inch iPad Pro is representative, you'll notice a short delay as Photos loads the raw file into memory, but you shouldn't notice any other difference in editing. Photos doesn't include any raw-specific editing tools, for instance.

There is a catch, if you shoot and import Raw+JPEG pairs (where the camera captures the raw file and also a separate JPEG image). In iOS, the Photos app edits only the JPEG portion, which may not be what you want. In Photos on the Mac, when editing a Raw+JPEG image, you can choose Image > Use RAW as Original to ensure that you're working with the raw version.

Editing iPhone Xs Portrait Images

The only other notable change in the editing features is support for the adjustable aperture feature for Portrait mode photos in the iPhone XS and iPhone XS Max. When editing a Portrait shot, a control appears below the image that makes the background more or less blurry, simulating the effect you'd see when shooting at wider or narrower apertures. Turned all the way to f/16, backgrounds are mostly crisp and in focus. When set to f/1.4, the widest setting, the background becomes more blurry to enhance the separation between it and the subject.



Only the iPhone XS models currently create the type of depth mask that this feature requires. However, the control does appear on some other iOS devices when editing a Portrait mode image captured with an iPhone XS or iPhone XS Max. I tested this with my iPhone X and 9.7-inch iPad Pro, and the control showed up; I don't have an iPhone 7 Plus or iPhone 8 Plus at hand, but I suspect it might work. It did not appear on my wife's iPhone SE.

A Parting Shot

Setting aside my criticisms, what I like about Photos in iOS 12 is Apple's acknowledgment that our digital photos shouldn't be stored away and forgotten as we chase the next image. Surfacing images in new ways and improving the search features keep us in touch with the reasons we took those photos in the first place. As our libraries increase in size, it's going to be more important to capture those moments, moods, and memories.

Software Review

Apple Updates

Security Update 2018-003 (High Sierra)
Dec 5, 2018 — 1.82 GB
System Requirements
– macOS 10.13

Security Update 2018-003 is recommended for all users and improves the security of macOS.

Security Update 2018-006 (Sierra)
Dec 5, 2018 — 828.4 MB
System Requirements
– macOS 10.12

Security Update 2018-006 is recommended for all users and improves the security of macOS.

macOS Mojave 10.14.2 Update
Dec 5, 2018 — 2.47 GB
System Requirements
– macOS Mojave 10.14.1

The macOS Mojave 10.14.2 update improves the stability, compatibility and security of your Mac, and is recommended for all users.

This update:

Adds RTT (real-time text) support for Wi-Fi calling

Adds a menu item to News for opening a story in Safari

Resolves an issue that may prevent iTunes from playing media to third-party AirPlay speakers.

macOS Mojave 10.14.2 Combo Update
Dec 5, 2018 — 2.52 GB
System Requirements
– macOS Mojave 10.14

The macOS Mojave 10.14.2 update improves the stability, compatibility and security of your Mac, and is recommended for all users.

This update:

Adds RTT (real-time text) support for Wi-Fi calling

Adds a menu item to News for opening a story in Safari

Resolves an issue that may prevent iTunes from playing media to third-party AirPlay speakers.

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