Dec 2017
Vol. XXVIII, No 11

KEYSTONE MacCentral

printout

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

December Meeting Features Our Traditional Holiday Party

The weather is cold, Christmas movies are playing on TV, and brightly colored lights adorn houses and trees. Obviously, Christmas is coming, and on December 19 KeyMac will be hosting our holiday party. The club will provide soft drinks and some snacks while Wendy Adams has volunteered to make her delicious chili. **We are requesting that you bring your favorite Christmas treats to share** so you can eat dinner and enjoy the evening's program 9 (some videos from Dennis) following the usual Q and A. Come out and mingle with your KeyMac friends on December 19th!

Meet us at

Bethany Village Retirement Center

Education Room
5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, December 19th 2017 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

Board of Directors

President
Linda J Cober

Recorder
Wendy Adams

Treasurer
Tim Sullivan

Program Director
Dennis McMahon

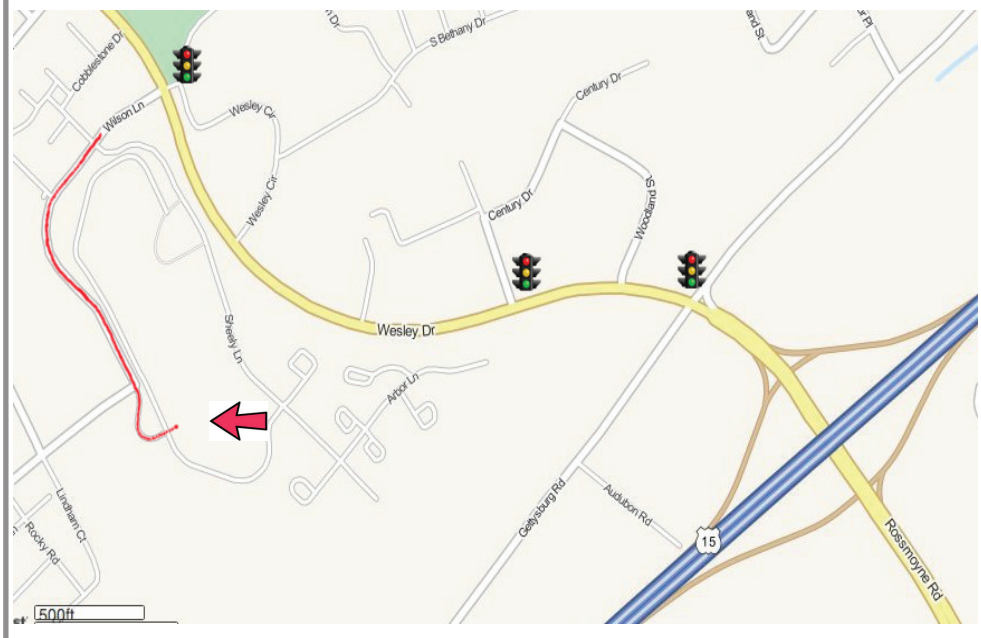
Membership Chair
Eric Adams

Correspondence Secretary
Sandra Cober

Newsletter Editor
Tim Sullivan

Industry Liaison
Eric Adams

Web Master
Tom Bank II



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

Five Major New Capabilities in Notes in iOS 11

iOS's bundled Notes app used to seem like a throwaway feature list item. With its skeuomorphic ruled paper, Marker Felt font, and sketchy syncing, it was worthwhile for only the most casual of uses. But Apple has focused a lot of attention on Notes for the past few iOS releases, and it has become my constant companion for everything from shopping lists to tracking changes for the "Take Control of iOS 11" manuscript.

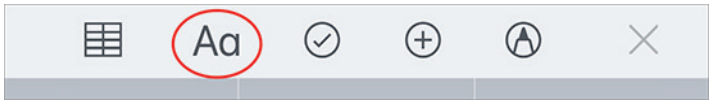
In iOS 11, Apple has again packed Notes with new features but hasn't promoted many of them other than Instant Notes, which I covered in "11 Things You Should Know about iOS 11" (20 September 2017). Here's what else is new in Notes in iOS 11.

Inline Sketching -- If you own an iPad Pro and an Apple Pencil, sketching inside a note is as simple as tapping the Apple Pencil on a large, empty spot. If you tap in the middle of some text, however, you'll just move the cursor.

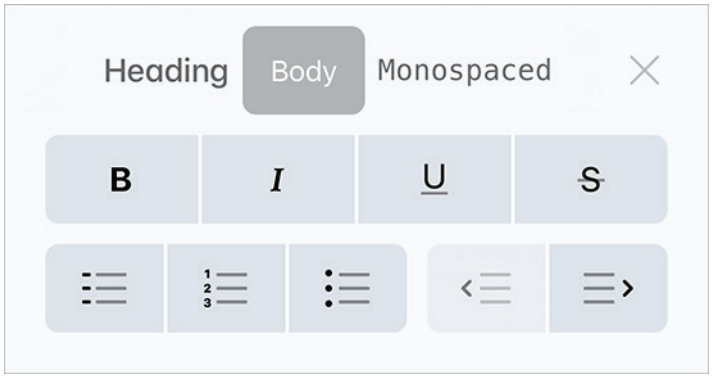
Notes indicates the sketching area with a yellow line at the top. Touch and drag the dot at the end of the line to move the content above the sketch up or down. Tap the Markup icon to see the full lineup of sketching tools.

If you want to get rid of the inline drawing entirely, tap in a blank area in the sketch and choose Delete from the pop-over.

Formatting Improvements -- Notes has offered simple text formatting for some time, but it was always clunky to use. In iOS 11, Notes presents most of its formatting options (apart from creating a checklist) in a single pane, accessible by tapping the new Aa button in the QuickType bar above the onscreen keyboard or on a standalone tool-bar if you have an external keyboard attached.

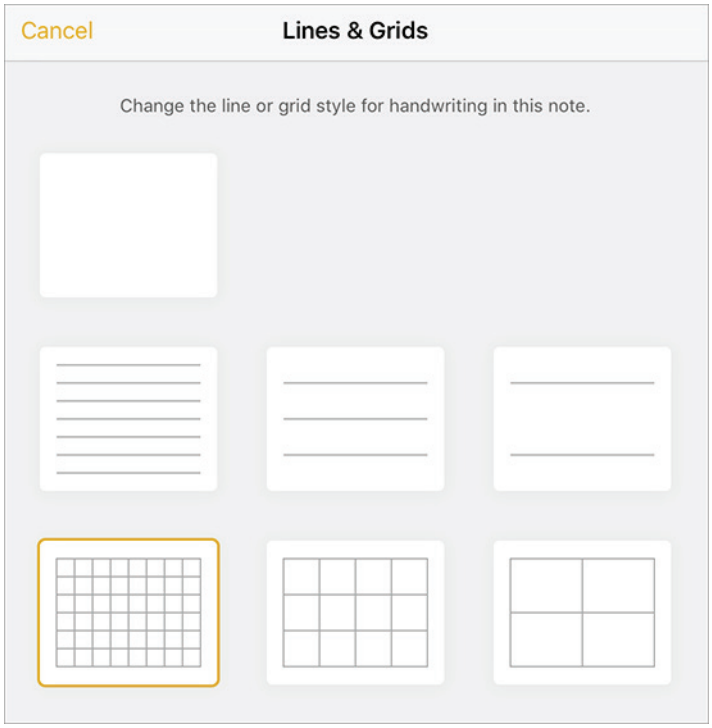


In addition to the body, heading, bold, italic, and underline styles, the pane offers two new styles: strikethrough and monospaced. From the formatting pane, you can also cre-ate bulleted, dashed, and numbered lists. Finally, buttons in this pane help you indent and outdent lists.



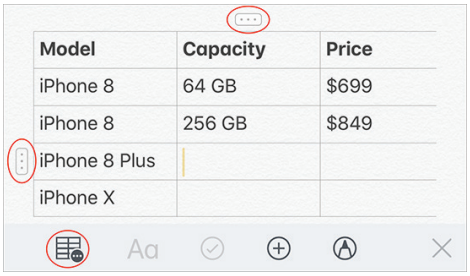
Unfortunately, indenting and outdenting list items doesn't change their markers, so it's not ideal for outlines. But here's a tip: you can now indent and outdent checklist items. That makes it possible to create hierarchical to-do lists, such as those used in the Getting Things Done system.

Another new formatting option in iOS 11 lets you choose the paper style of a note when using the Apple Pencil to write or sketch. To do so, tap the share icon while viewing a note and choose Lines & Grids, which gives you six different line and grid background options.



You can change the default handwriting background in Settings > Notes > Lines & Grids.

Tables -- Notes now lets you create simple tables. In a note, tap the table icon in the toolbar to create a simple two-by-two column. Tap inside a cell to edit the text there. When you do so, an ellipsis (…) button appears over the current column and next to the current row — tap one of those buttons to reveal options to add or delete columns and rows. You can also drag those buttons to move the associated column or row.



Here are a few more tips:

• When editing text in a cell, the Aa button is grayed out, but you can still format text by tapping in the cell to bring up the text popover, and then choosing BIU to reveal formatting options.

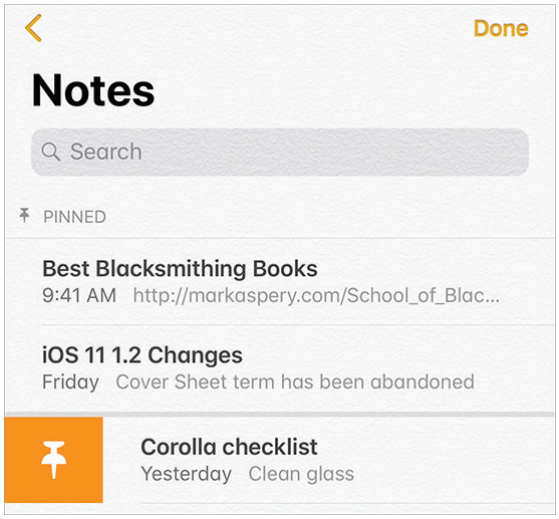
• While editing in the lower-right cell, tap the Next key to create a new row.

• While editing in a cell, notice that the table button now has an ellipsis over it. Tap it to copy, share, or delete the table, or to convert it to text.

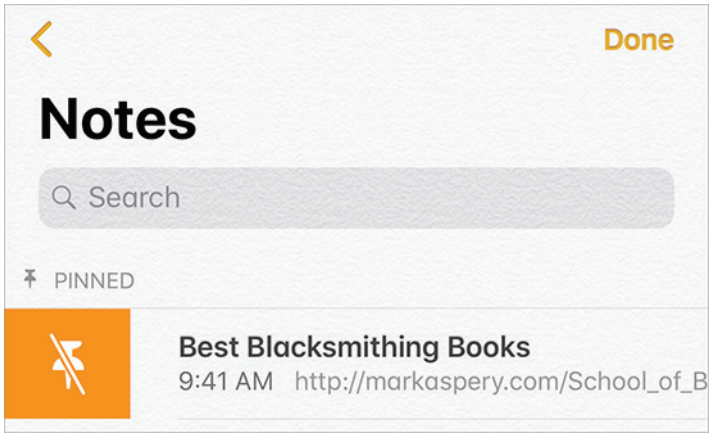
Alas, tables in Notes don't allow calculations or advanced sorting like spreadsheets in Numbers do.

Pin Notes -- Typically, Notes sorts your notes with the most recently edited ones at the top. In iOS 11, you can now pin specific notes so they remain at the top of the list.

To pin a note, right-swipe its listing to reveal a thumbtack icon. Tap that icon to pin the note. However, if you keep swiping the note listing after the thumbtack icon appears, you can pin it without tapping the icon.

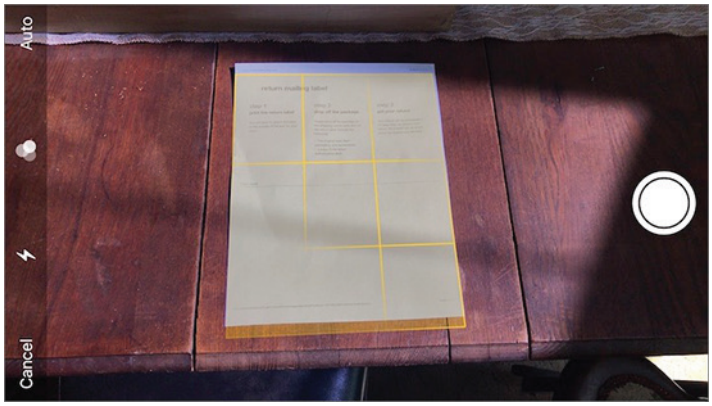


Pinned notes remain at the top of the list in the order you pinned them in. To unpin a note, swipe it right again to reveal a thumbtack icon with a line through it. Tap that button to unpin it or keep swiping to unpin it without tapping.

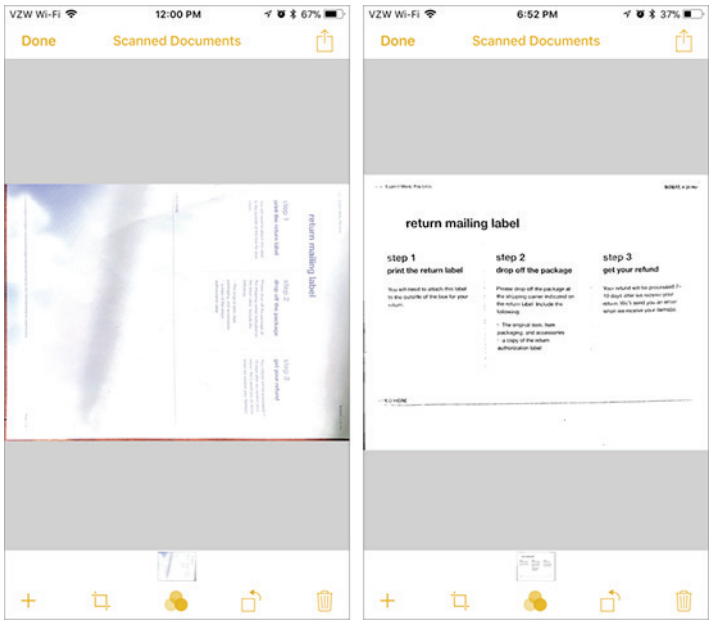


Document Scanner -- Over the years, apps like PDFpen Scan+ and Scanbot have become indispensable on the iPhone for quickly scanning documents. Those developers will have to up their games because Notes now has a document scanner built in. Lay a piece of paper on a flat, well-lit surface, and inside a note, tap the + button and choose Scan Documents. It's too bad you can't initiate scanning from the Camera app as well, since that's a more obvious location for such a feature.

The viewfinder will search for a document, and once it identifies one, it will automatically capture it. Controls at the top of the screen let you adjust the flash, choose color filters, and turn off auto capture if you want to press the shutter button yourself.



Notes lets you keep scanning documents into the same note until you tap Save. Scans are saved at the bottom of the note, and you can tap one to edit it right away. Editing controls let you crop, adjust color, and rotate it. In the screenshot below, I took a document I scanned in color, cropped the excess, converted it to black and white, and rotated it to portrait orientation. After saving, you can also tap the scan to edit it.



To share a scanned document, while it's open for editing, tap the share icon in the upper-left corner and choose Create PDF. From that view, you can mark up the PDF, or tap the share icon in the lower-left corner to send that PDF. I discuss marking up PDFs more in "Take Control of iOS 11."

There are two ways to mark up a scan while viewing it. The simplest is to tap an Apple Pencil to the screen of an iPad Pro. The other way is to tap the share icon and choose Markup. You can use this to sign documents, among other things.

Notes doesn't have OCR capabilities like PDFpen Scan+ and Scanbot, and it certainly won't replace a quality scanner, like a Fujitsu ScanSnap (a TidBITS sponsor), but if you only need to scan the occasional document, its handy scanner feature may be more than adequate.

Overall, Notes may not have a feature set that's competitive with something like Evernote or other long-standing note-taking apps, but it has sufficient capabilities for most everyday situations, especially if you have an iPad Pro with an Apple Pencil. The new features in iOS 11 make Notes worth a second look, if you don't already have a note-taking app you love.

by Glenn Fleishman

With a Stolen iCloud Password, Your Mac Can Be Held Hostage

Apple designed macOS's Find My Mac feature to help those who have lost a Mac or had one stolen recover their machines while simultaneously rendering the computers inaccessible. Unfortunately, Find My Mac has recently been subverted by extortionists relying on usernames and weak passwords leaked from account breaches at major sites like Yahoo and LinkedIn — not iCloud itself.

These criminals log in to iCloud.com with a leaked username and password, lock your Mac via Find My Mac with a secret code, and then post a message on the screen telling you where to send Bitcoin to receive the numbers to unlock your Mac.

If you have fallen victim to this attack, **do not pay** the ransom! Instead, go to an Apple Store or independent Apple Authorized Service Provider and — according to Apple's FAQ — with proof of purchase in hand, Apple can unlock your Mac. But change your iCloud password first.

You would think that Apple's two-factor authentication (2FA) would block this attack, but it doesn't, for the simple reason that Apple lets certain iCloud activities take place without a 2FA code. That's an intentional security decision that Apple made to allow people to lock lost devices even if they couldn't gain access to a trusted device or phone number — imagine that your Mac and iPhone are both stolen. But given how extortionists have subverted Find My Mac, Apple needs to rethink this feature immediately.

If you use the same password for iCloud and other sites or if you haven't changed your iCloud password in years, **change it immediately**. Some pundits are recommending that you disable Find My Mac, but doing that removes a valuable tool for data protection and device recovery. The password is the issue, not the Find My Mac service.

To see if your credentials may have been exposed in one of these major account breaches, you should also consult Have I Been Pwned?, a trustworthy site run by Australian security expert Troy Hunt that compiles public account breaches.

This attack doesn't work against iPhones and iPads that already have a passcode in place because iOS's Lost Mode relies on the passcode to unlock the device. But if your iOS device lacks a passcode or if you have a Mac, the Lock (Mac) and Lost Mode (iOS) in iCloud.com's Find My iPhone screen allow an attacker to enter a code only they know and display a custom message telling you how to pay up.

In addition to online reports and our testing, we have a direct report of this attack. A graduate student at Cornell (whose mother is a TidBITS reader and got in touch with

us) fell prey to this attack this week. Both of the student's MacBooks were locked, and a dialog appeared on her screens with an email address intended to appear as though it belonged to Apple.

Luckily, she had both Time Machine and Carbon Copy Cloner backups. Instead of responding to the email address, she called Apple and was told to take her MacBooks to the nearest Apple Store. (It's an hour away, and they couldn't fit her in for three days; just because Apple can help doesn't mean it will be convenient.) Upon doing so, and proving ownership with receipts, the Apple Store employees were able to unlock both computers. And the student's mother managed to refrain from admonishing her daughter for ignoring parental advice to use strong passwords and not reuse them across sites.

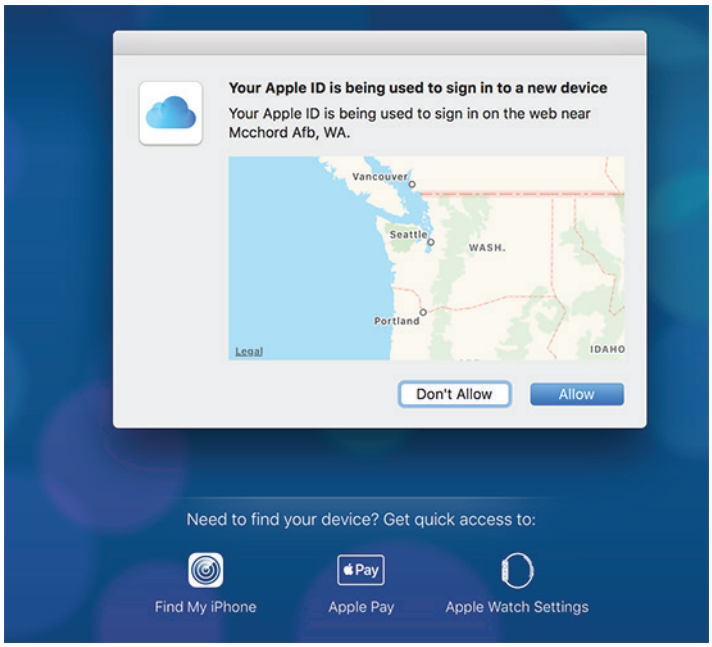
That's all you need to know. However, if you want to understand why these attacks are happening now, read on.

A Feature Becomes a Bludgeon -- To be crystal clear, iCloud has not suffered a major breach. Rather, this attack was made possible thanks to breaches at other sites that revealed usernames and passwords. The problem stems from people using the same password on both iCloud and a site that was breached. Since nearly five billion accounts have been exposed in breaches over the years, it's entirely likely that the bad guys have your credentials from those snapshots.

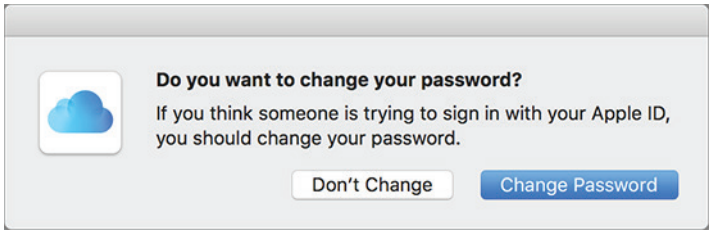
You would think an attack relying on reused passwords would already have happened to iCloud, and it has: many iCloud users had problems a few years ago when weak passwords in early breaches were cracked. The thing is, crackers are still churning away at stronger passwords from those exfiltrated databases using ever more powerful computational engines. Thus, passwords that might have withstood cracking in the past are falling to this continued effort. Plus, because Apple now actively encourages two-factor authentication, some people still rely on relatively weak passwords due to the belief that 2FA will protect them. That's actually a reasonable assumption — except in this one terrible case!

2FA does prevent someone with just your password from gaining full access to your iCloud. What criminals have realized more recently is that they can still wreak havoc on accounts that have crackable passwords, regardless of 2FA.

At iCloud.com, a login attempt for a 2FA-protected account begins with a request for the username and password. Next, on all 2FA-enrolled computers and devices, a prompt appears that asks the user to Allow or Don't Allow the login attempt. But here's the hole. Without dismissing that dialog, iCloud.com allows someone to access Find My iPhone, Apple Pay, and Apple Watch Settings, and from the Find My iPhone screen, lock a Mac or put an iOS device in Lost Mode. Apple should address this vulnerability immediately.



(Pay attention if you ever get an unexpected 2FA login request because it could indicate that someone has obtained your password. Whenever you receive an unexpected request, immediately disable Find My Mac on your Macs, change your iCloud password, and then re-enable Find My Mac. Also note that Apple recently changed what happens when you click Don't Allow. Formerly, nothing happened. Now, on the device from which you clicked Don't Allow, you receive a warning that someone might be trying to access your account and suggesting that you change your password.)



The other reason these attacks are happening now is that the spread of ransomware has popularized the notion of locking someone's files in exchange for payment. Such payments can be difficult to track to their recipients, thanks to Bitcoin, a largely anonymous cryptocurrency that can be readily used internationally and is the coin of the realm for illegal and dubious transactions. (Yes, Bitcoin is used for plenty of legitimate transactions, too, but it's the preferred medium for online black markets.) And before you ask, yes, Apple could track the IP addresses from which the Find My iPhone locking requests originate, but with VPNs, Internet cafés, and other ways to obfuscate origin, that wouldn't help.

We believe that attackers won't be able to erase your Mac or iOS device if you have 2FA enabled because erasure requires your second factor. We tested this with iOS but weren't able to confirm the final steps with macOS, not having a Mac we could erase on hand. Nonetheless, the same process appears to be followed. (Apple doesn't

document these erasure steps to that degree of granularity, which would help.)

Improve Your iCloud and General Password Security -- The summary of our best advice for your iCloud password and security, and for password hygiene in general, is as follows:

- Use a password manager. We use 1Password and LastPass around TidBITS. You can also use iCloud Keychain more extensively in iOS 11, which allows third-party apps to tap into an iCloud Keychain password store.

- Create a unique password for each site. With a password manager, this is trivial, both for creating them and filling them in.

- For services like iCloud, Google, and Netflix where you may need to type your password instead of using a password manager, use long passwords that are easy to type. The old advice — which many sites enforce, unfortunately — of using short passwords (often just 8 to 12 characters) with a mix of letters, numbers, and punctuation is outdated. The latest recommendations, including those promulgated by the National Institute of Standards and Technology, say longer, memorable, and easy to type is better. Password managers can create those for you, too.

- Enable 2FA everywhere you can, including iCloud. While this attack exploits a loophole in Apple's use of 2FA, 2FA retains its advantages everywhere else.

For more advice on password selection, using password managers, and general account security, consult Joe Kissell's excellent "Take Control of Your Passwords."

Thanks to high-profile breaches, many sites have dramatically increased their password-encryption security. Any intelligently run company has shifted to using better algorithms and approaches for encrypting passwords. Many sites now choose an algorithm that has a scaling factor — over time, the site can keep dialing a number up to keep stored passwords infeasible to crack despite increases in computing power. 1Password, LastPass, and others already use this technique to protect their vault passwords. In 2015, LastPass suffered a severe breach, but there were no reports of cracked accounts because of the computational burden to break through even a single password.

What we don't know is whether users are now regularly choosing better passwords and not reusing them across sites. The popularity of 1Password and LastPass would point toward some improvements there, but I'd argue that the outdated password requirements presented by many sites have kept less-savvy users from increasing password strength. Sites need to get with the times, follow best practices, and give users the best modern advice (which is coincidentally less frustrating, too).

Apple Needs To Rethink This Loophole -- Letting someone with just an iCloud password lock a Mac with a secret code seems like a bad idea. Perhaps Apple could change macOS's behavior to mimic that of iOS, which lets you unlock a device with the passcode. What if you could regain access to a Mac locked via Find My Mac using one of its macOS administrator passwords?

Apple could adapt a feature already used with FileVault 2 to enable such a capability while still allowing Mac owners who had just lost all their 2FA-enrolled hardware to lock their devices.

With FileVault, Apple uses the Recovery partition to store account information for all macOS logins that have FileVault access. When you turn on or restart a FileVault-protected Mac, macOS actually boots into Recovery. Entering your password unlocks the full-disk encryption key used for your main boot partition and allows the startup sequence to proceed normally.

Right now, however, if you don't have FileVault enabled, the Recovery partition has no account credentials that it could compare against when unlocking a Mac. That's likely why Apple lets the person locking a Mac choose the secret unlock code. If Apple updated macOS to store encrypted credentials for an administrator account in the Recovery partition, it would become possible to unlock a locked Mac with just the administrator password, just as in iOS, where the passcode disables Lost Mode.

With such an update, Mac users wouldn't have to worry about being extorted through iCloud password reuse, social engineering, or any other lost password scenario. We hope Apple is working to make this change or something similar.

by Rich Mogull

You Can't Protect Yourself from the Equifax Breach

Earlier this month, news broke of a massive data breach at Equifax, one of the three major credit rating agencies. Equifax may have lost private information, including Social Security numbers, for up to 143 million U.S. consumers, which would be over half of the adult, bank-account-participating population of the country. Some information from British and Canadian citizens may also have been exposed. In Equifax's own words:

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents.

Equifax subsequently botched its response and communications with consumers, including unclear legal clauses when you check your exposure, failing to provide specific information or an effective way to determine if you are affected, and even hosting its response Web site on a non-Equifax domain name using an incorrect digital certificate.

Ignoring all that, the real issue is that one of the companies "trusted" with determining our financial future based on deep records of personal information was breached… and due to the current nature of our financial system, we can't effectively protect ourselves. Our best options offer only limited protection and come at a hefty cost, due in large part to lobbying by the credit rating agencies themselves.

As a cybersecurity advisor, I have worked with companies in all the nooks and crannies of the financial system. While most take their responsibility very seriously, they are still businesses filled with humans working with a hodgepodge of a system that has developed over decades, if not centuries. Mistakes will happen, and our system is poorly designed to protect consumers.

Here is how to understand your risk and best live with the exposure.

Nine Digits to Rule Them All -- Banking and credit has always been a history- and reputation-based industry. Financial institutions provide credit but need some level of assurance they will get their money back. For hundreds of years, this was managed through personal relationships. Over the past few decades, however, society decided to prioritize faceless transactions and frictionless credit. Financial institutions no longer have direct relationships with their customers, and in many cases have never even met their customers. To manage their risk, these institutions started to rely on credit ratings developed by private companies dedicated to collecting and analyzing our financial histories.

Thus the emergence of credit rating agencies (CRAs) like Equifax, Experian, and Transunion. These companies collect everything from public records to your credit card payment history and use that information to determine those all-powerful credit scores. Credit scores are merely a single numeric risk rating that financial institutions can use to decide what type of credit to extend to you — from mortgages to credit cards — and for how much.

Since names aren't unique, the CRAs rely heavily on Social Security numbers (SSNs) as the unique identifier for individuals, sometimes in combination with full name and date of birth. The problem is that our system treats an SSN as a secret key to our financial records, but an SSN is merely a nine-digit number that is most definitely not encrypted.

SSNs are nearly impossible to change, are prone to errors, and clearly cannot be kept secret. Some bad guys first stole mine from a database at the student healthcare clinic where I went to college, and then it was exposed again (probably to China, based on public reports) during the big breach of the Office of Personnel Management (OPM) in the U.S. federal government.

In each of these cases, I was offered a year of free credit monitoring, just as Equifax has done in this latest breach. However, the free credit monitoring lasts only for a year, yet the bad guys can use my SSN for the rest of my life.

That's the real issue here. Once your SSN has been exposed, you can never be assured it will be secret or safe ever again. Data like your SSN and date of birth won't change, even after your death. Credit monitoring will only alert you to some kinds of new account fraud, essentially throwing a notification when someone creates a new account that is reported to a CRA. Those alerts won't necessarily notice when utilities or other services create accounts that also rely on your SSN.

Even if you can protect your financial records, loss of your SSN and other personal information could expose nearly any kind of account you have, not just financial accounts!

Think of all the situations where something is "protected" with the last four digits of your SSN or a credit card. Breaches of a credit agency like this expose the master key to recover or access more than a few of your accounts.

Once you're exposed, you're exposed for life, not just for the year of free credit monitoring. At least until the system changes.

Your Best Financial Defense -- Although you can get, by law, a free copy of your credit report every year from each agency, doing so doesn't offer much protection. You would need to be diligent about checking annually and then go through the process of cleaning up any new account fraud that occurs. ("Hey Siri, remind me to check my credit report every year.") Doing so can be a difficult process since the system is built to protect the financial institutions, and CRAs are historically reticent to respond to consumer issues. Remember, the CRA's customers are banks, not you. You're the product.

The first step is to make things harder for a criminal to create new accounts in your name. There are two tools to do this, fraud alerts and credit freezes, but only one actually works. You can find information, phone numbers, and links on the U.S. Federal Trade Commission's Identity Theft Web site:

A fraud alert places a flag on your account for 90 days. During that time a business needs to verify your identity before it can create a new account in your name. There used to be companies that could automatically renew your 90-day alerts for you, but the credit agencies sued them out of existence, which was a travesty. So, if you want an indefinite fraud alert, you need to repeat the process yourself every time it expires.

Another option is a credit freeze, which locks your account completely. The CRAs may charge for this service, and you will have to enter a PIN code to unlock your account. A credit freeze prevents all access to your account, including credit checks, and thus may have unintended consequences (for example, background checks for employment). It's your best option for long-term security and doesn't expire, but it isn't ideal.

There is one more option, an extended fraud alert that lasts for 7 years but is generally available — thanks to federal law! — only if you have already been a victim of identity theft.

These techniques can help, a bit, but at a cost. Worse, they do nothing to protect non-financial accounts secured with your private information.

Living with Long-term Risk -- Until the system changes, there isn't much you can do beyond a credit freeze, and that comes with some negatives, especially if you need to apply for credit or a job. Perhaps this incident will spur some legislative changes. The odds are high that more than a few politicians are also now exposed, and self-interest is a powerful motivator.

We normal consumers must be hyper-aware of when our SSNs are used as a security control. Does your healthcare provider use your SSN to decide when to release medical data? Does your school system use it to release transcripts? Does your bank use it as an account recovery passcode?

In my experience, most of these organizations, even if they use the infamous "last four digits," also offer alternative PIN or verification options. Try to use those alternatives whenever possible, or at least understand and accept your risk.

The average person isn't necessarily at risk of having someone impersonate them to get medical records, but there are plenty of occupations and situations where that might be a concern, including politicians, journalists, and anyone in a divorce or child custody fight.

I first learned to live with this risk personally thanks to the OPM breach that exposed more than just my SSN. The real lesson came as part of a second breach, which revealed a wealth of personal history that I had submitted as part of a standard security form. It included every place I have ever lived, every country I had visited in the preceding 7 years, and the personal information of all my immediate family members.

Knowing this information is out there is… disconcerting. There's no way for me to know who has it now: likely some Chinese intelligence agency or underground criminal information exchange. It's not an everyday source of stress, but more of a low-level buzzing in the back of my head.

I have to assume anyone who really wanted to could get my SSN and possibly a bunch of other private information. So I do my best to protect myself and my family by enabling multi-factor authentication on accounts whenever possible, creating account recovery questions that are pseudo-passwords, and changing PIN codes so they aren't the last four digits of my SSN.

I write this as a so-called security expert who makes my living in this industry, and I know I still have plenty of vulnerable accounts and financial risk. Practically speaking, the vast majority of consumers, or even TidBITS readers, don't have the time, knowledge, or security diligence to protect themselves indefinitely.

Since Equifax is one of the primary sources of credit reports and knows exactly how fraud occurs and how our information is used, it is unconscionable that the company offers only a year of free credit protection to the people it has harmed through its negligence. It's equally offensive that Equifax continues to prevent the use of tools like persistent fraud alerts that could help reduce our risk.

As much as I hate to end on a sour note, the reality is that, until the system changes, until our financial lives are governed by something stronger than some short strings of plain text that never change, we have to keep our guard up and hope for the best. And hope is never part of security best practices.



by Jeff Carlson

Using Long Exposure in iOS 11's Photos App

Take a look at this photo:

I captured this image under bright, mid-afternoon light at Snoqualmie Falls, a popular tourist spot outside Seattle. The silky-smooth waterfall catches the eye because it's different: we know waterfalls are more textured and violent than this. And it's a pretty effect.

The usual way to get this shot is to mount your camera on a tripod and set a slow shutter speed (perhaps half a second or longer) so the image sensor records the light reflecting from the water over a period of time, not just a fraction of a second's worth. The tripod is necessary because you don't want the camera to move during that time, which would introduce blur. The other challenge with long-exposure photography like this is that the sensor records all the light in the scene, not just the waterfall, so you can end up with an overexposed image, particularly in the middle of the day.

There are ways to compensate. You can set the aperture to a high value (f/16 or f/22) to restrict the amount of light coming through the lens. The preview on your camera will be dark, but the buildup of light during the exposure makes the final image more balanced. However, very high apertures can cause distortion or softness on some lenses.

Another way to compensate would be to add a neutral density filter in front of the lens, which also restricts the amount of light hitting the sensor and makes longer exposure times possible. But you may not have a filter that's dark enough — again, especially in bright daylight conditions. Here's a photo I took using my Fujifilm X-T1 camera at 1/4 second using an aperture of f/8.0 and with a 0.9 neutral density filter (which lets in about 12 percent of light):

If I really wanted to get the shot using the X-T1, I could have doubled up two or three filters (I also have 0.6 and 1.2 filters in my standard kit), but that introduces severe vignetting and some softness.

So how did I get that first image?

I pulled my iPhone 8 Plus out of my pocket and took one exposure, handheld, with the Live Photos feature turned on. And then I applied Apple's new Long Exposure effect in the Photos app. That's it.

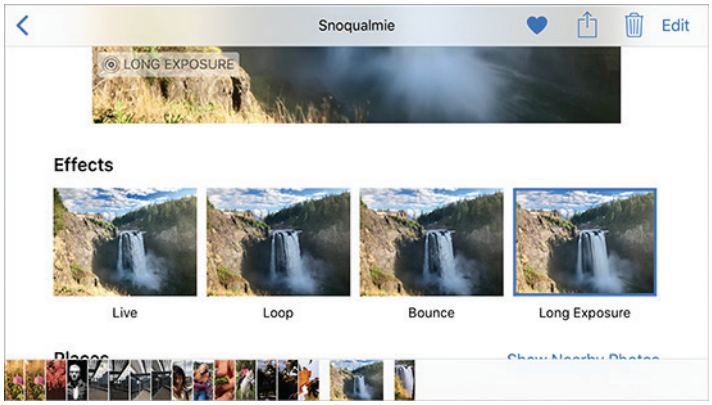
Here's the original image I captured, before I applied Long Exposure:

What's Going On? -- When you're using the Camera app on an iPhone or iPad, it continuously analyzes the scene and even records it, but does not save the footage. As soon as you tap the shutter button, the app evaluates the scene in milliseconds and delivers what it thinks is the best exposure for that moment. With Live Photos enabled, it also saves a video file containing 3 seconds of frames around that still image. Pressing and holding the image when viewing it in the Photos app plays back that video, giving you that Harry Potter-esque moving picture.

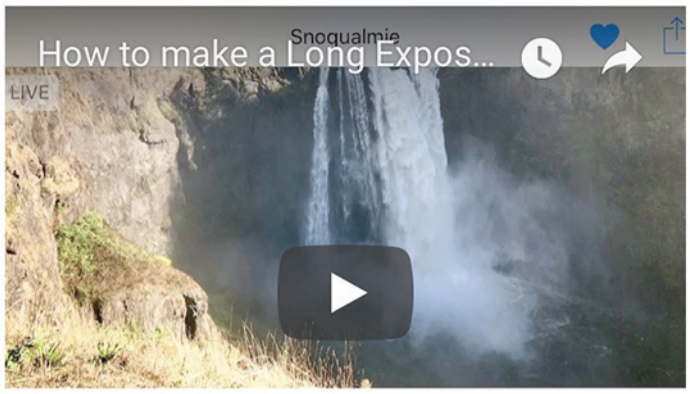
In iOS 11, Apple added three new effects that take advantage of the Live Photos video footage. Loop replays the video endlessly from beginning to end. Bounce plays the video start-to-finish and then reverses it to play finish-to-start, and back again as a loop.

The third effect is Long Exposure, which blends all the frames from the video into one image. It's the same principle as making a "real" long exposure by leaving the camera's shutter open for a relatively long period of time, but instead of just absorbing more light, it's combining the light in each of the frames. This happens algorithmically, which enables the app to keep the tones and detail in the sky and surrounding areas balanced.

The Long Exposure effect is dirt-simple to use. When viewing a Live Photo in the Photos app, swipe up to reveal more options, and choose Long Exposure under Effects.



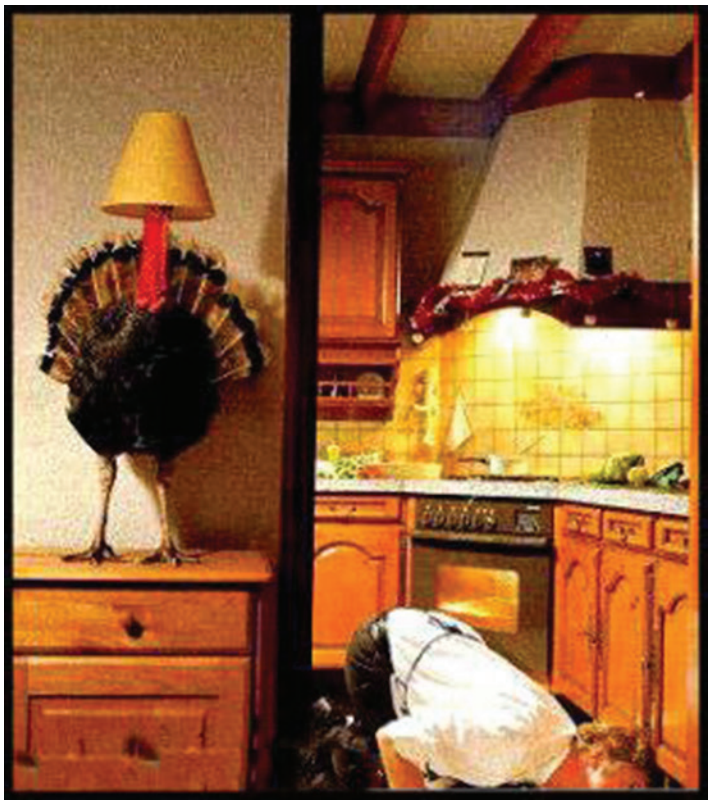
Here it is in action:



You can also apply the effect in Photos in macOS 10.13 High Sierra. Select the Live Photo, click Edit, and choose Long Exposure from the Effects pop-up menu (below the lower-right corner of the image).

Good as it is, the Long Exposure feature isn't perfect. If you zoom in and look closely, you'll notice that it loses a lot of detail in the rocks and sky compared to the original. It's fine on a small screen but doesn't stand up to scrutiny on larger displays. Applying Long Exposure also crops the image to account for camera movement; if you're intentionally capturing photos that will use any of the Live Photo effects, be sure to allow extra room around your subject.

Even so, I managed to capture a darn good long-exposure waterfall photo just by raising an iPhone and snapping a shot. As someone who has captured silky-looking waterfalls before, I know how much work is required to get them. And now everyone with an iPhone 6s or later running iOS 11 can get something very close to that with hardly any effort at all.



by Thomas R. Bank, II
Keystone MacCentral Webmaster

Of Hackintoshes and FrankenMacs

Apple has come a long way from its underdog days, relying on a band of dedicated followers for its business. Now it seems nearly everyone has or wants an iPhone. Although that would seem to be a good thing, one realizes the downside when one considers the roughly three-quarters of Apple's revenue coming from the iPhone and iPad and that the Mac isn't getting much attention these days.

One cannot deny the history of desktop Macs having an "all-in-one" form factor – back to the original Macintosh 128K on through the iMac G3 to the current iMac and Mac Mini and without much stretch to the MacBooks as well. But there are growing comments about compromises in performance due to form factor and weight. Where such compromises may make sense in a phone, tablet, or laptop, it makes little sense for a desktop. Even a laptop reaches a point where holding the title for "thinnest" or "lightest" may not win users if the performance doesn't measure up as well.

Yet alongside this all-in-one lineage of Macs there have also been the "modular" systems that one could easily argue descend from the original Apple][through the Macintosh II to Power Macintosh to the Mac Pro. These have had expansion slots, drive bays, easily accessible memory slots, and other amenities to allow users to build a Mac to suit their needs.

In 2010 Steve Jobs used a metaphor where he compared the future of computing to automotive terms and equated smart phones and tablets with lightweight commuter vehicles while computers (whether laptop or desktop) were the utilitarian trucks. He foresaw a shift where most of the public would likely only need a "commuter vehicle" for light computing use, yet there would always be those with the heavy lifting needs for a "truck."

Unfortunately, Apple's "truck" has suffered increasing neglect over the years. Since 2010, updates to the Mac Pro have been infrequent and much less changed from year to year. Whereas previous updates included current chip architecture and graphics options, 2010 and 2012 updates brought mostly speed bumps. Then, in 2013, the new Mac Pro (nMP) was reduced to an "all-in-one" form factor, locking users into expensive external options if the "one size fits all" didn't fit them. The only user-configurable components were memory and a single SSD. Although the GPUs are removable, there are no available options to replace them. So, with the nMP, Apple essentially welded the cargo doors shut on their "truck" and forced one to buy trailers (external drives, external graphic cards, etc) to "tow" any upgrades along behind.

Now, four years later, there have been no updates to the nMP other than minor price changes this past Summer, leaving the processors and graphics generations old. The 2010 Mac Pro has been obsoleted as well. Other than a discussion earlier this year that Apple was working on a "completely rethought" modular version of the Mac Pro, there have been no further updates on that front in the intervening six months.

Many might argue that an iMac or MacBook Pro is now powerful enough to take the place of a Mac Pro. In many cases, they may be right. Just as the "horsepower wars" have increased power and capacity of half-ton pickups to exceed that of one-ton pickups from a decade ago, MacBooks and iMacs have gained performance in recent years surpassing the old Mac Pros. Still, there are applications and uses where "one size fits all" just doesn't cut it – or, as the clothing industry puts it, "one size fits most."

One aspect not addressed by the all-in-one form factor is simple housekeeping. If your computer usage necessitates multiple hard drives to meet the storage needs for photography, graphics, or video files, having a tangle of cords leading to a pile of external units just gets messy. Add optical drives for backups or other peripherals and the "simplicity" of an all-in-one quickly disappears.

Graphics needs are another aspect not addressed by the all-in-one options. Viewing specifications for Apple's lineup shows only a few GPU options and no opportunity to upgrade or change them yourself. Further, even the iMacs and Mac Minis are using laptop GPUs to accommodate the required form factor at the cost of performance.

Whether GPU specs are needed for photo or video editing, 3D rendering, or gaming, chances are that up-to-date specifications and the ability to upgrade the GPU either as needs grow or to prolong the life of a computer are a requirement.

Further, some applications need a specific graphics acceleration framework for optimum results. To simplify, AMD uses OpenCL while Nvidia uses CUDA and Apple has been using AMD or Intel cards and chips, leaving applications using CUDA at a loss without Nvidia options.

This final issue is what brought me to search for upgrade options a year ago. The 3D rendering application, V-Ray by Chaos Group, that I use requires CUDA – and also will use as many GPUs as you throw at it to reduce render times.

None of Apple's offerings gave me CUDA acceleration. One option was to get a PCI-e expansion chassis that would connect to a Mac with a Thunderbolt cable, but a

single slot expansion chassis started about $200 and multi-slot chassis go into four digits. Another option was to admit defeat and move from the Mac to a PC solution, but that would mean changing my entire workflow to Windows applications or maintaining both Mac and Windows computers for separate tasks.

Ultimately, my solution was to modify a Mac to suit my needs. This would allow me to continue with my Mac workflow while offering the flexibility and components needed by that workflow.

People refer to these machines as Hackintoshes (hacked Macintoshes) or FrankenMacs (like Frankenstein, built from assorted components). They range from modest changes to "factory" hardware up to fully custom setups running OS X on PC motherboards and other components. Common elements include processor upgrades, graphic cards, and peripherals never offered by Apple and form factors outside of the iMac, Mac Mini, Mac Pro lineup.

Join us next month as I walk you through the considerations for my project, the components I chose, and how it all went together.

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