

**SOME WEBSITES**

Is iPad Pro A Laptop Replacement? Very detailed, well written, and thoughtful. [bit.ly/2pcwaih](http://bit.ly/2pcwaih).

More information on iPhone 11s. [bit.ly/2p9cKdT](http://bit.ly/2p9cKdT).

How to Get Wi-Fi in Your Car. It might be easier than you think. [bit.ly/2nDHDH1](http://bit.ly/2nDHDH1).

How To Subscribe To A Magazine Or Newspaper On The iPad. Download your favorite content and read it anywhere and on any device. [bit.ly/2olyKSr](http://bit.ly/2olyKSr).

How to Remove Your Personal Information From the Internet. Delete your public records from popular sites. [bit.ly/2ooh1cY](http://bit.ly/2ooh1cY).

Hands On Apple Watch Series 5. A couple of changes make a big difference. [bit.ly/2nuFeyv](http://bit.ly/2nuFeyv).

How to buy a refurbished Mac, MacBook, iPhone, or iPad from Apple. Want a new Apple device, but don't want to shell out for a full-priced version? [bit.ly/2nCTOUo](http://bit.ly/2nCTOUo).



FOUNDED MAY 1989

MEETINGS - SECOND

SATURDAY OF THE MONTH

## THE INTERNET OF THINGS

### NL FOCUS - 2 FACTOR AUTHENTICATION & REMINDERS

Our main speaker will be Fran Rabuck. Fran will cover general definitions and history of The Internet of Things (IoT) in markets like Home, Health, Buildings, Cities and some niche markets. Home and health might be the most interesting. He will also cover the world of wireless options. Fran will bring some IoT devices but it may be tough to setup demos depending on wifi.

**BIO:** Francis (Fran) Rabuck is a technology evangelist, explorer and trail blazer. He discovers trends, connects people, beta-tests things and then builds early prototypes of a mashup of ideas. He shares his findings in the classroom, workshops, presentations, articles and keynotes at a variety of international conferences. Fran is currently the Chief Strategy Officer for Agile Handover.

**OCTOBER LOCATION**

WE WILL AGAIN MEET AT THE EAST WHITELAND FIRE COMPANY, 205 CONESTOGA ROAD IN MALVERN. IT'S ON ROUTE 401. GO TO [MLMUG.ORG](http://MLMUG.ORG) FOR MAPS.

**CONTENTS**

Some Websites and Program Info	1
MLMUG and Newsletter Info	2-4
Bookmarks: iPad V. Laptop	5-8
September 14, 2019 Meeting Minutes	8-10
Speaker Roster 2019	10
How To Protect Your Identity Online	11-13
<b>Two-Factor Authentication for Apple ID</b>	<b>14-16</b>
How to Set Up Authy for Two-Factor Authentication	17-20
Stop Unsolicited Credit Card Offers	20
<b>Is the Reminders App A True Task Manager?</b>	<b>17-22</b>
Some Speaker Roster Details	22
If You Use the Reminders App a Lot,Read This Read This Before Updating to iOS13	23
Fix SPOD - How To Fix a Spinning Pinwheel of Death	24-26
<b>How To Save Old Photos to Your Computer</b>	<b>26-28</b>
How To Choose a Photo Scanner	28-29
The 7 Best Free Photoshop Alternatives	30-33
The 5 Best Photo Editor Apps of 2019	34-38
iPhone 11 and 11 Pro Review: Thinking Differently in The Golden Age of Smartphones	38-41
4 Search Tools To Find Email Addresses	42-44
AI and Humans: Defense Defense	45-46

**Contributors and Authors**

Apple  
 Mark Bazrod  
 Bradley Chambers  
 Brian X. Chen  
 Tim Fisher  
 Kathy Garges  
 Lory Gil  
 Stanley Goodner  
 William Harrel  
 Chris Hoffman  
 Dave Johnson  
 Elise Moreau  
 Tom Nelson  
 Scott Orgera  
 Surrey Services

**Newsletter Editor**

Mark Bazrod

**Graphics Editor**

Sally Bazrod

**Copy Editor**

Deane Lappin

**MLMUG Journal  
Masthead**

Designed by Dale Fletcher  
 Based on prior designs by  
 Marc Robinson, Steve  
 Evans & Bobby Foster

**MLMUG Journal** is  
 published monthly by the  
 Main Line Macintosh Users  
 Group and is available  
 online. It is produced using  
 Apple Pages with a  
 Helvetica Neue font (Same

**President, Program Director &  
Vendor Liaison**

Maria O. Arguello

[mariarguello@mac.com](mailto:mariarguello@mac.com)

**Vice President & Multimedia SIG  
Co-Chair**

Larry Campbell

[lcampbell9@me.com](mailto:lcampbell9@me.com)

**Treasurer, Membership &  
Facilities Coordinator**

Elliott Cobin

[eicobin@gmail.com](mailto:eicobin@gmail.com)

**Secretary & Newsletter Editor**

Mark Bazrod

[msb@pilease.com](mailto:msb@pilease.com)

**Educational Liaison**

Linda McNeil

[mcneil.linda@gmail.com](mailto:mcneil.linda@gmail.com)

**Member-at-Large, Newsletter  
Copy Editor & Apple User Group  
Ambassador**

Deane Lappin

[deanezl@verizon.net](mailto:deanezl@verizon.net)

**Multimedia SIG Co-Chair**

Nicholas Iacona

[nick@nickiacona.com](mailto:nick@nickiacona.com)

**Newer Users SIG Co-Chair &  
Webmaster**

Bob Barton

[barton@bee.net](mailto:barton@bee.net)

**Newsletter Graphics Editor**

Sally Bazrod

[sallybazrod@mac.com](mailto:sallybazrod@mac.com)

**OS/iOS SIG Chair**

Adam Rice

[adam@adamrice.org](mailto:adam@adamrice.org)

**Picnic Coordinator**

Tony DiPiano

[tony@dipiano.net](mailto:tony@dipiano.net)

**Raffle Chair**

Susan Czarnecki

[sparsefur@yahoo.com](mailto:sparsefur@yahoo.com)

**Social Secretary**

Gail Montgomery

[gailmontgomery@comcast.net](mailto:gailmontgomery@comcast.net)



**Apple  
User Group**

**Membership Information**

Membership dues are \$25 for individuals and \$35 for families. Memberships are based on your anniversary date, which is the month you joined. You will be e-mailed reminders when membership fee is due.

If you're just visiting to check us out, or if you've been visiting for some time, but haven't joined, consider these **BENEFITS OF MEMBERSHIP**:

- **Monthly meetings**, where you can learn, share, and meet everyone from working Mac professionals to new Mac users from all backgrounds.
- **Monthly newsletter**, which is full of interesting Mac news, tips, and information.
- Useful free items at the monthly **Raffles**.
- **Discounts**. Vendors offer special prices to User Group members.
- **Web Site** with 2-3 years of MLMUG newsletters, meeting information, a member directory, directions to our meetings, and much more! Our web site is [www.mlmutg.org](http://www.mlmutg.org).
- **MLMUG Mailing List**, to post technical questions or comments to each other and the experts within the group.
- **Reviewers** keep items reviewed.

Are you ready to join? Please make a check payable to MLMUG and bring it to a monthly meeting or mail it to:

Treasurer, MLMUG

P.O. Box 1374

Southeastern, PA 19399

## Typical Meeting Agenda

**9:00 - 9:05:** Call to order in main meeting room.

**9:05 - 10:05: Two Concurrent Special Interest Groups (SIGs)** convene in separate rooms. The two current SIGs are:

**Multimedia** - We discuss using your Mac/iDevices and applications for photo, video, audio, and print media.

**OS** - We go beyond basics to discuss Apple's current operating systems, using your Macs & iDevices, & various applications, & have Q&A.

**10:05 - 10:15:** Continuation of Q&A for all attendees.

**10:15 - 10:30:** Welcome and other business.

**10:30 - 11:50: Main Presentation** (by a member or guest)

## MLMUG Email list

The Main Line Macintosh Users Group has its own email list, hosted at [Groups.io](http://Groups.io). Compose your letter and email it to [MLMUG@groups.io](mailto:MLMUG@groups.io) and your message will be sent to everyone on the mailing list. Contact Bob Barton ([barton@bee.net](mailto:barton@bee.net)) if you are a member and you are not on the list.

Please observe good email etiquette. If your message is humor or not Apple-related (off-topic), please include "Humor" or "OT" in the subject line. The [Groups.io](http://Groups.io) Terms of Service are at [groups.io/static/tos](http://groups.io/static/tos). Look for the section on "Conditions of Use"

The MLMUG list may be used to post Apple-related items for sale, but any solicitation of members through the list is forbidden without the written consent of a MLMUG officer. Violation of the [Groups.io](http://Groups.io) terms of service or good email etiquette may result in removal from the list.

## New Users SIG

You don't have to wait a whole month to get answers to your basic Mac questions! Get together with other members on the fourth Saturday (i.e., two weeks after each regular meeting) for the Startup Folder Lite.

Many new users have said that they can learn much more from face-to-face meetings than they do from manuals or other sources. That's what this meeting is all about. Go to [www.mlmutg.org/nusfl.html](http://www.mlmutg.org/nusfl.html) for details.



## Bookmarks

By Mark Bazrod

### iPad v. Laptop

I wrote a column back in October 2015 on whether iPads will replace laptops. As the performance of iPads has increased every year and more commentators have been addressing the issue, it's probably time to update the column.

I particularly liked two articles - Cam Secore's *iPad Pro vs. MacBook Air: Is iPad Pro A Laptop Replacement? (2019)*, [bit.ly/2oznkdV](http://bit.ly/2oznkdV). It is well written, thoughtful, very detailed, and should be read by anyone considering buying an iPad or MacBook. Also, Daniel Nations' *Can an iPad Replace My Laptop or Desktop Computer?* [bit.ly/2nXm4RZ](http://bit.ly/2nXm4RZ).

I think the primary question is not whether iPads will replace laptops (including MacBook Airls and Pros), but whether iPads will replace or supplement laptops. There is no simple answer to that question.

The best approach is probably to split computer users into two groups - average users and advanced users (often called power users).

The average user's computing needs are primarily email, searching the web and perhaps storing photos. The advanced user's needs are much more and generally require more sophisticated and complex software and hardware.

The average user typically has a laptop, (although it doesn't matter whether it's a laptop or desktop) and perhaps an iPad. The advanced user typically has at least three or four devices - a desktop, a laptop, an iPad, and an iPhone.

Let's first look at the state of the iPad today, as exemplified by the iPad Pro, the top-of-the-line model of the iPad.

The iPad Pro is faster and more powerful than most MacBook Pros, not even to mention the MacBook Air and most other laptops. And Apple has sold more iPads in 4 years than it has Macs in 30 years.

Look at the comparison at the end of this column for more comparative information.

**FOR THE AVERAGE USER, THE IPAD AIR OR THE IPAD PRO IS MORE THAN ADEQUATE. THESE USERS SHOULD SWITCH TO AN IPAD!** They will avoid the complexity of Windows and Mac PCs. The problem is getting some people to change old habits is often an insurmountable barrier.

In addition, for many average users, the iPad mini is all that is necessary. Its much smaller size makes it a preferable device for many.

Although the iPad Pro is superior to the MacBook Air in many respects (certainly power), its somewhat limited storage, only one connector, and a less robust operating system, particularly an advanced file management system, make it less than a PC replacement for the advanced user. Also, some of the more important apps on the iPad, such as

Pages, Numbers, and Keynote, are decidedly less than full-fledged apps.

There are several hard drives which connect wirelessly to iPads so the storage limitation is somewhat alleviated and iPadOS will now allow hard drives to be directly connected to an iPad. Nonetheless, I think Files needs to be vastly improved before an advanced user can replace his laptop.

Tim Cook has stated that the iPad Pro is more powerful than 90% of the laptops that are currently available. The Motley Fool calls Apple's A10X chip a "ridiculous beast".

Now to the real issue - from the aspect of the advanced user.

To truly understand the issue you should read an outstanding 2012 article by John Kirk, *The PC is the Titanic and the Tablet is the Iceberg. Any Questions?*. [tinyurl.com/bokmvmv](http://tinyurl.com/bokmvmv). It appeared in techpinions.com. Macobserver's John Martellaro called Kirk's article the "the best article I've seen in a long time that explains the tablet phenomena".

Kirk wrote:

"...it isn't the few overlapping tasks that the PC and the Tablet can both do well that matters most. It is the tasks that the Tablet excels at - and which the PC does poorly or not at all - that will ultimately reduce the PC to niche status and turn the Tablet into the preeminent computing device of our time.

But let's be real. The PC is a better PC than the tablet is, or ever will be. The number of Tablets that will directly replace PCs will never amount to great

numbers. ....There are millions upon millions of Tablets that are supplementing, rather than replacing, the PC." [Editor underlining].

Kirk's point is that the iPad wins because it does many tasks that the PC doesn't. If you read Kirk's article, you'll be amazed at the number of tasks that iPads are currently performing and we have not yet begun to touch the iPad's full potential. Remember, there are armies of independent developers, businesses and users who see potential iPad uses we never imagined.

The truth is that the PC form factor has become a premium niche - for the advanced user (and the average user who resists change).

The advanced user determines which device he will use, depending upon the task to be performed. For high-performance computing he will use a desktop or a powerful laptop. But I have seen many instances where the apps on the iPad in particular situations are superior to desktop/laptop apps. I suspect that the number of iPad users has increased so much and the ease of marketing to iPad users through the Apple App Store is so much easier that many developers are focusing on the iPad market.

For text processing the advanced user can use any computing device, although for longer text processing we all tend to use a desktop or laptop. Advanced users are increasingly using their iPads, even in the office, and especially when they are away from their primary "computing station". What the iPad has done is to extend the range of computing.

Thus, the answer as to whether the iPad will replace the PC is an emphatic "it depends". For the average user, the iPad

should replace the PC, but inertia is often hard to overcome. For the advanced user, the iPad will be a supplemental device with its use depending upon the particular task. I suspect that as time progresses and iPads become more

powerful, have more storage, and have more connections to peripherals, an increased amount of computing will shift from traditional devices to iPads. It would not be at all surprising to see that what we now think of as laptops will end up being some form of iPad.

For an excellent comparison of the iPad Pro and the MacBook Air, read the following material from Cam Secore's *iPad Pro vs. MacBook Air* article.

## iPad Pro

**Speed:** It's faster and more powerful than most MacBook Pros.

**Operating System:** It runs the same OS as iPhone, which is great, but limiting when you want to do real work.

**Security:** It uses multi-orientation Face ID to unlock and it works brilliantly.

**Screen:** The touchscreen looks amazing and smoothest on the market and the design is the best Apple's ever made.

**Keyboard:** It utilizes a touchscreen with the option of a keyboard case.

**Uses:** It's perfect for games, movies, drawing web browsing. And OK for document writing if it's not regularly needed.

## MacBook Air (2018)

**Speed:** It's not as fast or powerful as iPad Pro, but it's 10x more capable.

**Operating System:** It runs macOS. The possibilities are limitless, and the apps are more advanced compared to iPad Pro.

**Security:** It has Touch ID on the top right-hand corner of the keyboard.

**Screen:** The design feels and looks brilliant. The screen doesn't get as bright or clear as iPad Pro.

**Keyboard:** There's no touchscreen, but there's a real keyboard and convenient trackpad.

**Uses:** You can create or consume as much as needed without hiccups. It's only a half-pound heavier than a 13-inch iPad.

## September 14, 2019 Meeting Minutes

### By Mark Bazrod, Secretary

Maria Arguello, our President, opened the MLMUG meeting at about 9:10 AM at the Ludington Library in Bryn Mawr. There were about 30 attendees.

### Q & A Panel - Adam Rice, Nick Iacona, and Bob Barton, with occasional .help from Mike Inskeep.

Dave Wolf asked a question about syncing files between his Mac and Apple's iCloud. This led to an extended and excellent discussion about working with iCloud.

Apple's recent approach has been to get the average user to put more of his files on the iCloud. In general, your files are put on iCloud, but can also remain on your Mac.

To save files on iCloud, go to *System Preferences > iCloud*. If you click on the *iCloud Drive > Options* box, you will also see the list of apps which can be saved on iCloud. More importantly, if you check the *Desktop and Documents* box, all your files on the Desktop and in the Documents folder (but not Movies, Music and Pictures) will be copied to iCloud Drive. The first 5 GB are free. 50 GB cost \$1 per month; 1 TB, \$10 per month.

If you do not check the *Optimize Mac Storage* box, the full contents of iCloud Drive will be stored on your Mac. If you do check *Optimize Mac Storage*, your Mac will store all eligible files in iCloud Drive, and may remove them from your local storage if you don't have enough local space to store everything.

You cannot use iCloud Drive to boot your Mac. For back up, use SuperDuper or Carbon Copy Cloner. They are excellent. Free and premium versions are available.

Apple encrypts files sent to iCloud with the password on computer. So that's another reason to use a strong password for your computer!

If you are concerned about additional security for some files, you should encrypt or password protect them. If you have files you do not want stored on iCloud Drive, you could put the docs in a folder outside the Documents folder. However, Mike says don't save documents outside the Documents, Music or Pictures folders because you don't have permissions protection.

**Q & A.** The new iPadOS will allow adapters for outside storage, including SD and MicroSD cards. Some older iPads may not have hardware for this option.

**Q.** How do I stop getting notices to upgrade NTFS?

**A.** NTFS can be read by both Windows and Mac PCs. NTFS drives are not bootable. You need to reformat to HFS+. You may have to first update NTFS or contact the manufacturer. Also check login items.

**Q.** Can I stop the iPad from always asking for my password when I open it?

**A.** No.

**Q.** What ad blockers do you recommend? And I sometimes have to disable them with some websites.

**A.** Having to disable is not unusual. Just reload the site after you disable. Adam likes 1Blocker or Ka-Block for Safari on macOS. Mike recommends uBlock Origin and Privacy Badger (by the Electronic Frontier Foundation) for a Mac

and 1Blocker for iOS. Also, Apple Safari Reader Mode turns off ads for most web sites.

Don't use Adblock. It is run by a marketing company which makes money charging advertisers to not block their "acceptable ads."

**Q. & A.** You often will see paywalls for a webpage which will limit you to perhaps five or 10 articles a month. Many of us pay \$50 or \$100 a year to have unlimited viewing.

Browsers have a Reader View which allows you to view the content of a webpage without ads and other stuff. To enable, just click on the little hamburger icon (3 or 4 horizontal bars) somewhere near the top of the page. Ads can be bobby trapped with malware. Check Safari > Privacy to manage cookies.

**Q. & A.** Open PDF files in Preview rather than Adobe Reader.

### **FileMaker Presentation. Jeff Gorman.**

There are two kinds database – flat, such as Excel, and relational, such as FileMaker.

Flat databases have a grid of rows and columns. They are excellent at mathematical complications, but can be a pain if there are many different kinds of data. Many users use flat databases a good bit of the time. Relational databases have a multitude of tables which are related to each other and are used to manipulate data much more than doing math. Once you learn to use them, they can be much easier to use than flat databases.

FileMaker 18, the newest version, has lots of templates. For the purpose of a presentation, Jeff finds it easier to start

fresh. My impression is that is often the case. He showed us how to begin to make a database for a veterinary practice.

Tables are similar to a spreadsheet. The first table was for clients (owners). Jeff started with some necessary fields, such as the client's name and email address. There are many field types, including text, date, time, timestamp (date and time), container (holds files, PDF), age, summary, and a few more.. He set up separate fields (columns) for first name and last name. He next examined what properties to assign to each field, such as auto enter, not empty, OK if empty, and email addresses must have an @ sign. There are tons of formula functions for specifying form.

You use Layout Mode to arrange the screen. Comments can be entered for directions, as can error messages. Standard fields can be copied. Each record (row) has a unique primary key. You don't want blank fields. Rather, set up a new table. He performed a calculation to have a full name field - first name plus last name. It's important to remember to type in information one time so you refer back to the first time the data was entered. No retyping! You should try to prevent mistakes by using properties for a field..

As you work, you can switch between Layout and Browser Mode to see what the screen looks like.

Jeff then set up a new table for pets. The general rule is to set up a separate table for a separate thing. Pets are certainly different from clients. He changed the primary key name to Pet primary key to make it more readable. Properties of the Pet Table were name, not empty, must enter, kind or species, make sure enter certain words, member of value list - dog, cat, frog, birth date, use date field rather than text, make as restrictive as you can, less

than or equal to today, minimize errors, change to pop-up menu, add to list, and allow editing of a list.

The next step is establish a relationship between the tables. Copy the Client Key into the Pet Table. There is a chart of the tables. You only have to draw a line between the Client Keys in the two tables to link them.

There is also a portal tool which show tables which are related and with which you can add data to main table. You can make a pet record from Client Table. Looks very powerful.

There is an app, FileMaker Go, which you can use on the iPad. However, you can't change the database from the iPad. There is no charge for the app.

The cost of FileMaker is \$399. You need 5 licenses to show FileMaker on the web.

Security. Who can enter data. Restricted privileges.

There are FileMaker consultants, including Jeff. His email address is jeffgorman@iteasy.us. His phone number is 609.427.3279.

---

### SPEAKER ROSTER FOR MLMUG'S 2019 MEETINGS

January 12	Nick Iacona - Mojave & iOS 12 Walkthrough
February 9	Jeff Porten - Productivity
March 9	Mark Bazrod - Search Strategies and Resources
April 13	Dave Comeau - 3D Projectors & New Technology
May 11	Dave Hamilton - Backup Strategies
June 9	Picnic
July	Recess - Summer
August	Recess - Summer
September 14	Jeff Gorman - Create a FileMaker Database On The Fly
October 12	Fran Rabuck - Internet of Things
November 9	Bob "Dr. Mac" LeVitus - TBA
December 8	Pot Luck Brunch, Members' Show &

Dave Johnson posted the following article to [howtogeek.com](http://howtogeek.com) on September 25, 2019. [bit.ly/2mUO7Ru](http://bit.ly/2mUO7Ru). © How-To Geek, LLC. He is a tech author (about 3 dozen books), editor, tech magazine contributor, and serial podcaster.

## How to Protect Your Identity Online

By Dave Johnson



When Sandra Bullock starred in *The Net* in 1995, identity theft seemed new and unbelievable. But the world has changed. Starting in 2017, nearly 17 million Americans are victims of identity fraud every year.

### Identity Theft Is Serious

Identity crimes include scenarios like a hacker who steals your credentials to break into your accounts or assume your financial identity, or someone thousands of miles away from you who runs up charges on your credit card and takes out loans in your name.

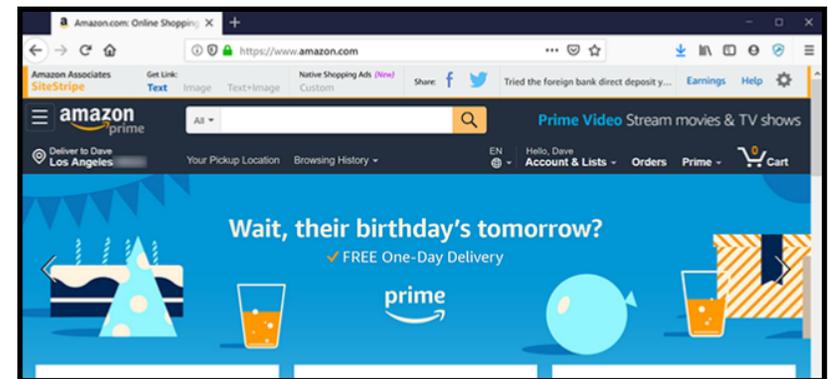
If you need something else to keep you awake, the [FTC describes identity theft scenarios](#) in which a thief gets a credit card in your name, sends the bill to another address, and (of course) never pays. Or he uses your personal information to steal your tax refund or pretends to be you if he's arrested.

It can be hard to untangle yourself from identity theft, both legally and financially. And the damage to your credit history can be long-lasting. If there ever was a scenario in which an ounce of prevention is worth a metric ton of cure, this is it.

### How Your Identity Can Be Stolen

Unfortunately, your identity is low-hanging fruit, able to be plucked in tons of ways. Offline, criminals steal mail from mailboxes or dumpster dive through trash, both of which might be chock full of credit offers and personal finance information (which is why you should own a shredder). Skimmers connected to gas pumps can capture your credit card info and so can restaurant staff. And recently, a cashier was arrested for stealing 1,300 credit cards he'd memorized.

Online, it's even more dangerous, but people are increasingly more savvy to the most egregious hacks. Fewer and fewer unsecured retail web sites (those that begin with "http" rather than "https") conduct transactions, but it's still something to keep in mind.



This requires ever-more subtle phishing campaigns to trick people into giving up their personal information via credible-looking fraudulent emails. And there's always a new scam around the corner.

“Another popular scam is through online dating apps,” said Whitney Joy Smith, president of The Smith Investigation Agency. “Scammers look for vulnerable people to build a relationship. After that, they ask for money or get enough personal information to conduct identity fraud.”

And then there are plain old hacks, such as when databases full of personal information are cracked.

### **How You Can Protect Yourself**

“Unless you’re willing to take extraordinary measures, like abandoning all technology and relocating to the Amazon to live with an uncontacted tribe, real privacy is almost impossible to achieve,” lamented Fabian Wosar, chief technology officer at Emsisoft. But Wosar also acknowledged there are reasonable and pragmatic precautions people can take.

Many of these are part of the usual cybersecurity hygiene you’ve heard for years. But to be truly be protected, you need to do these things, and regularly. After all, identity theft is usually a crime of convenience and opportunity, so your goal is to make yourself the smallest target possible.

And while the more precautions you take, the better, the reality is not everyone is going to be ultra-diligent. With that in mind, we’ve separated the precautions you should take into three levels: Common sense (the stuff everyone should be doing), heightened security (for the savvier), and bunker-mentality (for those who are willing to take extreme measures).

### **Common Sense Precautions**

If you’re not doing these things, you might as well stop locking your front door and leave your unlocked car idling in your driveway:

**Use strong passwords:** The conventional wisdom is that a strong password is some combination of upper- and lowercase letters, numbers, and special characters. The reality is the longer

your password is, the harder it is to crack. XKCD did a good job breaking it down.

**Use a unique password for every site and service:** This should go without saying, but it’s still routine to encounter people who re-use passwords. The problem with this is if your credentials are compromised on one site, it’s trivial for hackers to retry those same credentials at thousands of other sites. And according to Verizon, 81 percent of data breaches are possible due to compromised, weak, or re-used passwords.

**Use a password manager:** A tool like Dashlane or LastPass is table stakes in the games of online security. According to Dashlane, the average internet user has over 200 digital accounts that require passwords. And the company expects that number to double to 400 within the next five years. It’s pretty impossible to manage that many strong, unique passwords without a tool.

**Beware of public Wi-Fi:** Don’t join a free public Wi-Fi network unless you’re certain it’s trustworthy. You could join a network set up exclusively to monitor your traffic. And if you use a public or shared computer (such as to print a boarding pass when you’re on vacation), make sure you don’t allow the browser to remember your credentials—clear the cache when you’re done.

### **Heightened Security**

As the saying goes, you don’t have to run faster than the bear; you just have to outrun your buddy. If you implement these security best practices, you’ll be well ahead of the majority of the online population:

**Never use your social media profile to sign in to other sites:** When you sign up somewhere new, you often get a “single sign-on” option to log in with your Facebook or Google account. While this is convenient, one data breach exposes you in multiple ways. And “you risk giving the site access to the personal information contained in your sign-on account,” warned Pankaj Srivastava, chief operations officer of the privacy

company FigLeaf. It's always better to sign up with an email address.

**Enable two-factor authentication:** This effectively prevents bad actors from using a password reset to take control of your accounts. If you require two factors, they need access not just to your email account, but to your phone, as well. And you can do better than this, too (see the bunker advice below).

**Minimize your social media footprint:** Social media is an increasingly dangerous landscape. Also, don't accept connection or friend requests from anyone you don't know. Bad actors use that as an opportunity to research a phishing campaign, or she might use you as a jumping-off point to attack your contacts.

**Dial back your social media sharing:** "The more you post about yourself, the more a hacker can learn about you," said Otavio Friere, chief technology officer at SafeGuard Cyber. "And the more effectively you can be targeted." There might be enough information on your Facebook profile right now (email address, school, hometown, relationship status, occupation, interests, political affiliation, etc.) for a criminal to call your bank, pose as you, and convince a customer service rep. to reset your password. Simon Fogg, a data privacy expert at Termly, said: "As well as avoiding using your full name and date of birth on your profile, consider how all your information connects. Even if you don't share your home address, your phone number could be used to find it. When combined with geotagged photos, you might be surprised how much of your daily life you're revealing to strangers, and how vulnerable you have made yourself to threats."

## Into the Bunker

There's no end to the security precautions you can take—we didn't even cover using a TOR browser, for example, or making sure your registrar keeps the WHOIS information on your website (if you have one) private. But if you already do everything we

mentioned in the previous sections, these remaining precautions should put you in the top one percent of safe internet users:

**Never use your phone number for two-factor authentication:** "Phones can be cloned," said Initial Coin Offering (ICO) consultant, Steve Good. That makes your second factor in two-factor authentication less secure than you might think. Thankfully, it's easy to set up Google Authenticator or Authy to consolidate all of your two-factor-authentication needs.

**Encrypt your USB flash drives:** How do you transfer files between computers? With flash drives, of course. And these devices are often the weak link in your security regimen. If you lose it, anyone can pick it up and read it. You can encrypt individual files, but a better solution is to encrypt the entire device. Kingston offers a family of drives—the DT2000—that range from 8 to 64 GB. They have built-in numeric keypads, and protect your data with hardware-based, full-disk AES, 256-bit data encryption—no software required.

**Use a Virtual Private Network (VPN):** When you use this type of network, you connect to the internet (at least somewhat) anonymously. It's especially useful when you connect to public Wi-Fi, but there could be merit in using it at home, as well. "A VPN disguises your IP address and location," said Srivastava. "So, it looks like you're browsing from a completely different location. You could be at a local café in Boston, but others will think you're browsing from Sydney, Australia, or wherever you've chosen to virtually connect from." However, you might want to look for a VPN that doesn't maintain logs, as they can identify you and your online activities.

**Monitor yourself:** "Periodically reviewing your online presence will help you discover how much of your personal information is public," said Fogg. It's easy to create Google alerts for yourself which can help you get a sense of what the internet knows about you.

---

December 7, 2018 Apple posted the following article to [apple.com](http://apple.com). [apple.co/2nHrS1s](http://apple.co/2nHrS1s). © Apple Inc.

## Two-Factor Authentication For Apple ID

Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password.



### How it works

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information—your password and the six-digit verification code t

hat's automatically displayed on your trusted devices. By entering the code, you're verifying that you trust the new device. For example, if you have an iPhone and are signing into your account for the first time on a newly purchased Mac, you'll be prompted to enter your password and the verification code that's automatically displayed on your iPhone.

Because your password alone is no longer enough to access your account, two-factor authentication dramatically improves

the security of your Apple ID and all the personal information you store with Apple.

Once signed in, you won't be asked for a verification code on that device again unless you sign out completely, erase the device, or need to change your password for security reasons. When you sign in on the web, you can choose to trust your browser, so you won't be asked for a verification code the next time you sign in from that computer.

### Trusted devices

A trusted device is an iPhone, iPad, or iPod touch with iOS 9 and later, or a Mac with OS X El Capitan and later that you've already signed in to using two-factor authentication. It's a device we know is yours and that can be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser.

### Trusted phone numbers

A trusted phone number is a number that can be used to receive verification codes by text message or automated phone call. You must verify at least one trusted phone number to enroll in two-factor authentication.

You should also consider verifying an additional phone number you can access, such as a home phone, or a number used by a family member or close friend. You can use this number if you temporarily can't access your primary number or your own devices.

### Verification codes

A verification code is a temporary code sent to your trusted device or phone number when you sign in to a new device or browser with your Apple ID. You can also get a verification code from Settings on your trusted device.

A verification code is different from the device passcode you enter to unlock your iPhone, iPad, or iPod touch.

## Set up two-factor authentication for your Apple ID

Two-factor authentication is available to iCloud and iTunes users with at least one device that's using the latest iOS or macOS. Learn more.

You can follow these steps on your iPhone, iPad, or iPod touch to turn on two-factor authentication.

### Turn on two-factor authentication in Settings

If you're using iOS 10.3 or later:

Go to Settings > [your name] > Password & Security.

Tap Turn On Two-Factor Authentication.

Tap Continue.

If you're using iOS 10.2 or earlier:

Go to Settings > iCloud.

Tap your Apple ID > Password & Security.

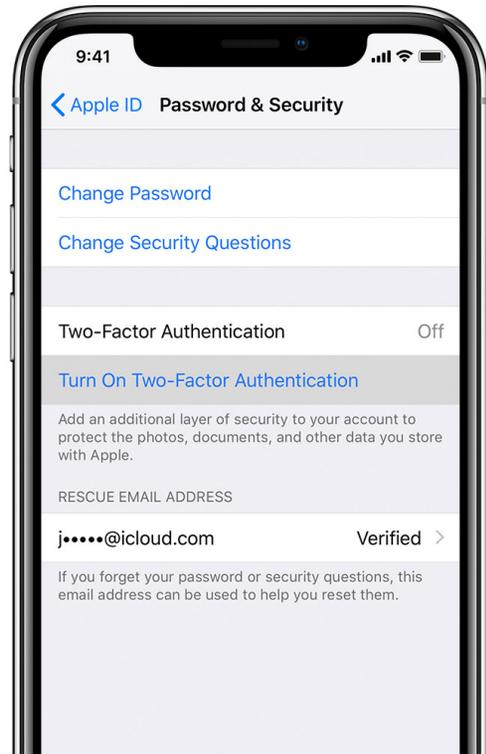
Tap Turn On Two-Factor Authentication.

Tap Continue.

You might be asked to answer your Apple ID security questions.

### Enter and verify your trusted phone number

Enter the phone number where you want to receive verification codes when you sign in. You can choose to receive the codes by text message or automated phone call.



When you tap Next, Apple sends a verification code to the phone number you provided.

Enter the verification code to verify your phone number and turn on two-factor authentication.

### Follow these steps on your Mac with OS X El Capitan or later:

Go to Apple () menu > System Preferences > iCloud > Account Details.

Click Security.

Click Turn On Two-Factor Authentication.

Some Apple IDs created in iOS 10.3 or macOS 10.12.4 and later are protected with two-factor authentication by default. In this case, you see that two-factor authentication is already turned on.

If you already use two-step verification and want to update, [turn it off, then turn on two-factor authentication](#).

If your account isn't eligible for two-factor authentication, you can still use [two-step verification](#) to protect your information.

### What to remember when you use two-factor authentication

Two-factor authentication significantly improves the security of your Apple ID. After you turn it on, signing into your account will require both your password and access to your trusted devices or trusted phone number. To keep your account as secure as possible and help ensure you never lose access, there are a few simple guidelines you should follow:

- Remember your Apple ID password.
- Use a device passcode on all your devices.
- Keep your trusted phone number(s) up to date.
- Keep your trusted devices physically secure.

## Manage your account

You can manage your trusted phone numbers, trusted devices, and other account information from your Apple ID account page.

## Keep your trusted phone numbers up to date

To use two-factor authentication, you need at least one trusted phone number on file where you can receive verification codes. Consider verifying an additional trusted phone number other than your own phone number. If your iPhone is your only trusted device and it is missing or damaged, you will be unable to receive verification codes required to access your account.

You can update your trusted phone numbers when you follow these steps:

1. Go to your Apple ID account page.
2. Sign in with your Apple ID.
3. Go to the Security section and click Edit.

If you want to add a phone number, click Add a Trusted Phone Number and enter the phone number. Choose to verify the number with a text message or automated phone call, and click Continue. To remove a trusted phone number, click next to the phone number you want to remove.

## View and manage your trusted devices

You can view and manage a list of your trusted devices in the Devices section of your Apple ID account page.

1. Go to your Apple ID account page.
2. Sign in with your Apple ID.
3. Go to the Devices section.

The device list shows the devices that you're currently signed in to with your Apple ID. Select a device to view the model, serial number, and other useful information, including whether or not

the device is trusted and can be used to receive Apple ID verification codes.

You can also remove a trusted device. Removing a trusted device will ensure that it can no longer display verification codes and that access to iCloud, and other Apple services on the device, is blocked until you sign in again with two-factor authentication. If you need to find or erase your device before you remove it from your trusted device list, you can use Find My iPhone.

## Generate app-specific passwords

With two-factor authentication, you need an app-specific password to sign in to your account using third-party apps or services such as email, contacts, or calendar apps not provided by Apple. Follow these steps to generate an app-specific password:

Sign in to your Apple ID account page.

Click Generate Password below App-Specific Passwords.

Follow the steps on your screen.

After you generate your app-specific password, enter or paste it into the password field of the app as you would normally.

## Frequently asked questions

Editor - Go to the posted article to read the many questions. [apple.co/2nHrS1s](https://apple.co/2nHrS1s).

---

Chris Hoffman posted the following article to [howtogeek.com](http://howtogeek.com) on July 3, 2017. [bit.ly/2nTZHMP](http://bit.ly/2nTZHMP) © Demand Media. He is Editor in Chief of How-To Geek and has personally written over 2,000 articles at How-To Geek. He has written articles for many magazines and has appeared on TV.

## How to Set Up Authy for Two-Factor Authentication (and Sync Your Codes Between Devices)



### By Chris Hoffman

Strong passwords are not enough anymore: we recommend using two-factor authentication whenever possible. Ideally, that means using an app that generates authentication codes on your phone or a physical hardware token. We prefer Authy when it comes to authentication apps—it's compatible with all sites that use Google Authenticator, but is more powerful and convenient.

### Why You Should Generate Codes With Authy (and Not SMS)

Two-factor authentication requires you have both the password for your account and an additional authentication method. That way, even if someone were to find out your email, Facebook, or other password, they'd need an additional code to sign in.

SMS is one of the more common ways to get these codes, but SMS is inherently insecure. It's too easy to intercept SMS

messages, which means someone with the know-how could get not just your password, but your two-factor codes as well—leaving your accounts vulnerable.

That's why we recommend using an authentication app. Instead of sending you a code when you try to log in, these apps are constantly generating new codes that are only valid for about 30 seconds each. When you're logging into an account and prompted for a code, you can just open your authentication app, grab the most recent code, and paste it in.

Google Authenticator is one of the most commonly recommended apps for these codes, and it's fine—it's just a little too basic. When you get a new phone, your Google Authenticator codes can't come with you. You'll need to set up all your accounts all over again. If you've lost your previous phone, you may need your backup recovery codes to regain access to your account and disable the authentication.

Authy offers a more polished app that avoids these hassles. Authy lets you back up your two-factor authentication codes to the cloud and to your other devices, encrypted with a password you provide. You can then restore that backup to a new phone, or if your phone isn't nearby, use your computer or your tablet to generate codes instead.

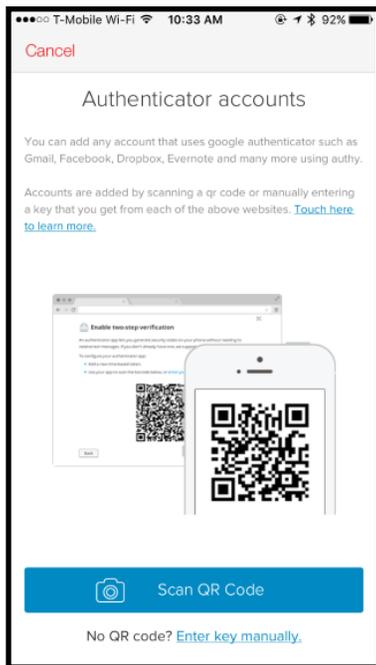
Here's the most important part: Authy is completely compatible with Google Authenticator. Whenever a website directs you to scan a QR code with Google Authenticator to set up two-factor authentication, you can scan the same code to set up two-factor authentication in Authy. That means you can use Authy anywhere Google Authenticator is accepted—for example, with your Google, Microsoft, and Amazon accounts. Some sites offer Authy-specific integration, too, so it really works everywhere.

### How to Use Authy

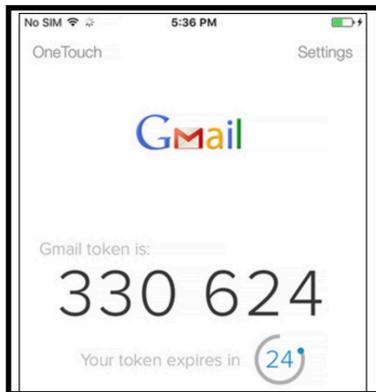
Authy is simple to use and free. Android users can download it from Google Play, while iPhone and iPad users can get it from Apple's App Store.

Once you've installed the app, enter your mobile phone number and email address. You'll be sent a PIN, which you'll enter to confirm you have access to the phone number.

Authy is now enabled. You just need to visit the two-factor authentication setup page on your account service of choice and pull up a QR code as if you were setting up a new Google Authenticator app. After you do, tap the "Add" button in the drawer at the bottom of the Authy screen and scan the QR code. The account will be added to Authy.



When you need a code, open the Authy app and tap the account you need a code for. Type the code into the service. There's also a quick copy button here, in case you want to paste the code into another app on your device.



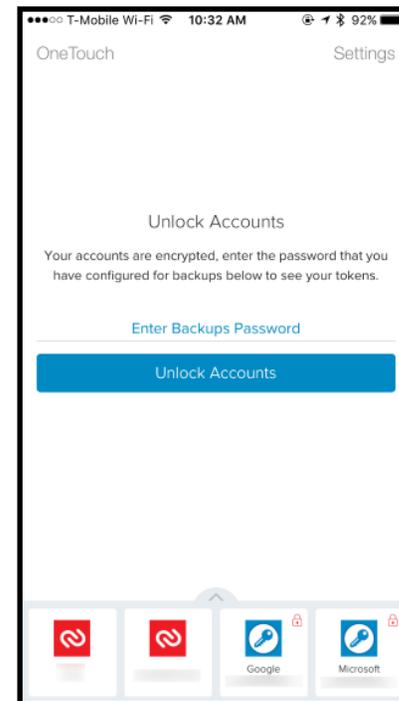
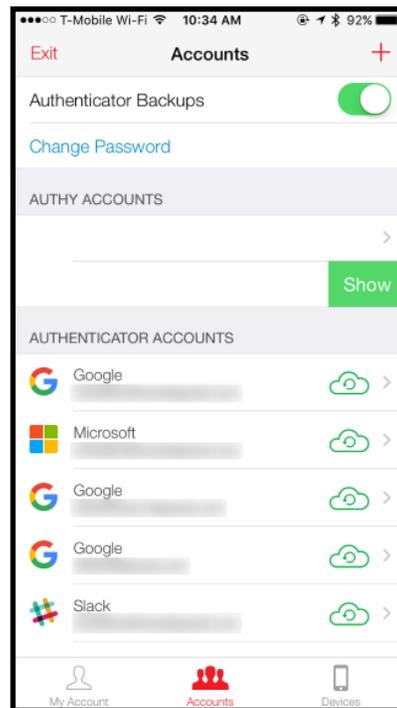
If you want to prevent people with your phone from easily gaining access to your codes even after you've signed in, you can enable as protection PIN (or Touch ID on an iPhone) from Settings > My Account > Protection PIN.

## How to Back Up and Sync Your Authy Codes

Authy can automatically create encrypted backups of your account data and store them on the company's servers. The data is encrypted with a password you provide.

You don't have to enable this if you don't want to! If you just want to use Authy on a single device and not store anything in the cloud, go ahead and skip this feature. Authy will store your codes only on your device, just like the standard Google Authenticator app. However, you won't be able to recover your codes if you lose your phone. You'll have to set everything up from scratch again. We recommend using Authy because of these features.

Open Authy and tap Settings > Accounts. At the top of the screen, ensure "Authenticator Backups" is enabled. You can use the password link to provide a password that you'll need to decrypt the backups. You'll need this password to access your codes when you sign into Authy on a new device.



Authy can sync your codes across multiple devices, too. For example, Authy offers a Chrome app that allows you to access your codes on any computer. There's also a macOS app in beta and a Windows app coming soon—you'll find them all on Authy's downloads page. Or, you may just want to sync your codes between a phone and a tablet. It's up to you.

To add other devices to your account, head to Settings > Devices in Authy. Enable the "Allow Multi-device" switch.

Now, try to sign into Authy with another device—for example, via the Authy Chrome app or an Authy mobile app on another device. Enter your phone number, and then you'll then be prompted to authenticate with an SMS message, a phone call, or through a prompt in the Authy app on a device you've already signed in with.

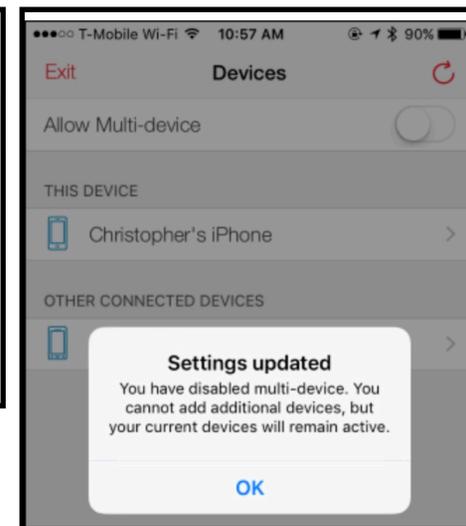
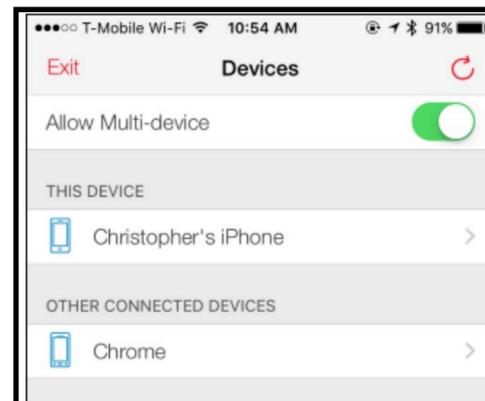
If you authenticate, the device you sign in with will gain access to your accounts. However, you won't immediately gain access to your codes. If you've set up a backup password to encrypt your codes in the cloud, you'll see a lock icon next to each of the codes you have in Authy. You'll need to enter your backups password to actually access the codes.

Note that the password only applies to Google Authenticator-style accounts. Accounts using Authy's own two-factor authentication scheme will be available after you sign in, whether or not you know the backups password. Authy's own two-factor authentication scheme really just checks whether you have access to a phone number.

Any changes you make to your codes—such as adding or removing an account—will now be synced to your other devices. Your list of devices will also appear on the Settings > Devices screen in Authy, and you can remove any devices you like from here.

Once you've added all the devices you want, head back to Settings > Devices in Authy and disable the "Allow Multi-device" option. The multi-device sync feature will keep functioning

normally, you just won't be able to add new devices. This is a good thing, since adding devices uses SMS—which, as we already discussed, is insecure. So you only want to turn this option on if you're adding a new device. Then disable it afterwards.



Note, however, if you disable multi-device and need to sign in on a new device—for example, perhaps you only had Authy on your phone and your phone was lost, damaged, or stolen—you won't be able to do so. You'll see a message saying multi-device is disabled and you need to re-enable it.

If you only had Authy on a single device and you no longer have access to that device, you won't be able to access your codes. Authy has an account recovery form you'll need to use, and it may take 24 hours before you get a response. This will wipe all the devices from your account and allow you to start over. However, if you've backed up your data, you'll be able to provide your backups password and regain your codes afterwards.

Authy officially recommends adding two (or more) devices to your Authy account and then disabling the “Allow multi-device” feature. No one will be able to gain access to your account until you re-enable multi-device. If you lose access to one device, you can always re-enable multi-device and add a new device.

However, if you just have a single device, you may want to think twice before disabling the multi-device feature. This will make it more difficult to access your code backups if you ever lose access to your single device.

For more technical details, read Authy’s official blog posts about the [multi-device feature](#) and [how backups work](#).



*Jacqlyn Kennedy Sisson wrote the following article for Surrey Services August Newsletter Personal Finance Corner. She is Surrey’s Personal Finance Manager. [bit.ly/32Zdxwx](http://bit.ly/32Zdxwx).*

## Stop Unsolicited Credit Card Offers

**By Jacqlyn Kennedy Sisson,**

One of the best ways to protect yourself from fraud is to reduce the amount of pre approved credit card offers you receive either in the mail or via electronic communications. If one falls in the wrong hands, it can be used to create a fake account for fraudulent purchases.

One way to control these types of offers is to visit [www.optoutprescreen.com](http://www.optoutprescreen.com) Opting out of prescreened card offers makes it less likely that an ID thief will intercept them and take out credit in your name.

OptOutPrescreen.com is the official Consumer Credit Reporting Industry website to accept and process requests from consumers to Opt-In or Opt-Out of firm offers of credit or insurance.

You can opt out for five years electronically or by calling 888-567-8688. Better yet, you can mail in a form to block pre-screened offers permanently. You may still receive offers from companies you currently do business with such as your bank or mortgage lender.



Bradley Chambers posted the following article to [9to6mac.com](https://9to6mac.com) on August. 18, 2019. [bit.ly/2oKo4wZ](https://bit.ly/2oKo4wZ). He manages Apple devices for a private school in Chattanooga, TN.

## Is The Reminders App Ready To Be Considered A True Task Manager In iOS 13 And MacOS Catalina?

By Bradley Chambers



I made the decision a few weeks ago to install the beta of macOS Catalina. It's still pretty buggy, but since I enjoy testing out new features (and writing about them), I am willing to deal with the crashes and incompatibility throughout the summer. One of the biggest surprises for me has been the changes in the Reminders app. Over the years, I used several to-do/GTD/project management/task apps. From Kindless GTD, Omnifocus, Things, and Todoist, I've used a lot of them. I've always looked at the Reminders app with interest, though. It's hard to beat the advantages of a built-in-app. With macOS Catalina and iOS 13, the Reminders app is finally ready to take its place alongside the rest of the task apps on the Apple ecosystem.

### New design

Over the years, Reminders has looked more like a simple list app than an actual task app. Even as the iOS design was simplified, Reminders still slightly resembled its pre-iOS 7 design. iOS 13 and macOS Catalina brings an entirely new design to the Reminders app. It's the first significant overhaul of the Reminders app I can remember since version 1. The new design allows you to better organize your tasks and projects where the previous version felt like it was useful for making a simple grocery list.

In the redesigned Reminders app, there are four main sections. They include Today, Scheduled, All, and Flagged. These sections will pull in tasks from all of your lists whether they are personal or work-related.

### New features in iOS 13 and macOS Catalina

Back June of 2018, I wrote an article about some features that I wanted to see Apple add to Reminders. One of them was sub-tasks, and Apple made it a reality in 2019. By dragging tasks under each other, you can create nested tasks. This feature will allow you to get more organized with more complex projects.

While iOS 13 and macOS Catalina didn't bring a share sheet to Apple's Mail app, you can now share text from an email into the Reminders app, and the app will associate the tasks with the email so you can easily pull it back up when you go to work on the task. You can do the same thing with websites, maps, etc.

Natural Language input is something I relied on with Todoist, and Reminders is also adding support for it. While the natural language support is not as robust as some of the other apps, you can now type things like Call Bob tomorrow, and Reminders can process that as being due tomorrow. When it comes to task entry, this is something that can speed up your work.

## Wrap-up on Reminders in iOS 13 and macOS Catalina

I am thrilled to see Apple putting work into the Reminders ecosystem this year, and I hope it continues in the future. I'd love to see more robust attachment support and the ability to forward a task via email (with a random iCloud generated email address). Apple set the groundwork in 2019 for Reminders to get a lot better in the future. Are you running the betas of the new Apple operating systems? What do you think about the upgraded Reminders app? Let me know in the comments.

---



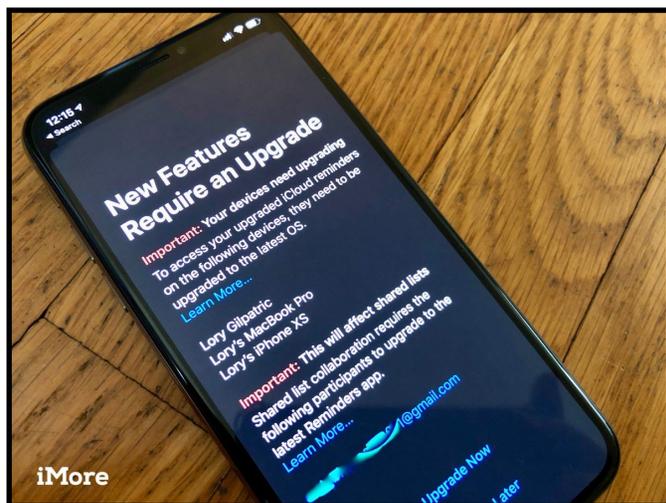
### SOME SPEAKER ROSTER DETAILS

- February 9 - Jeff Porten** - An author of several Take Control eBooks.
- March 9 - Mark Bazrod** - Long time MLMUG member, presenter, and Newsletter Editor.
- April 13 - Dave Comeau** - Long time MLMUG member and entrepreneur.
- May 11 - Dave Hamilton** - Co-founder of The Mac Observer and publisher and co-host of the Mac Geek Gab Podcast
- June 9- Picnic** - Valley Creek Park, Route 29, East Whiteland
- September 14 - Jeff Gorman** - Apple Specialist , PMUG member; and owner of Creative Computing in New Hope, NJ.
- October 12 - Fran Rabuck** - Technology/Strategy Research Analyst, Visionary Communicator and Futurist
- November 9 - Bob "Dr. Mac" LeVitus** - a leading expert on Apple products and software. Has written or co-written more than 85 popular computer books. Known for his trademark humorous style and unerring ability to translate "techie" jargon into usable and fun advice for regular folks.
- December 14 - Pot Luck Buffet, Member's Show and Tell, and Election of Officers for 2020** - An opportunity to enjoy friends, and good food, A "Show and Tell" session.

Lory Gil posted the following article to [imore.com](http://imore.com) on September 19, 2019. [bit.ly/2mrc42x](http://bit.ly/2mrc42x). © Mobile Nations. She is a renaissance woman, writing news, reviews, and how-to guides for iMore.

## If You Use The Reminders App A Lot, Read This Before Updating To iOS13

Reminders in iCloud and shared reminders all need to be on the latest operating system so consider this before installing the iOS 13 Reminders update.



### By Lory Gil

If you're ready to mash that install button and update your iPhone to iOS 13, there is one thing you should be aware of before you jump into the new features of Reminders — you can't update iPadOS 13 or macOS Catalina until later and iCloud Reminders in iOS 13 won't sync until they do.

The biggest sync issue is with iCloud. If you update Reminders to iOS 13, but your iPad isn't running iPadOS 13 or your Mac isn't

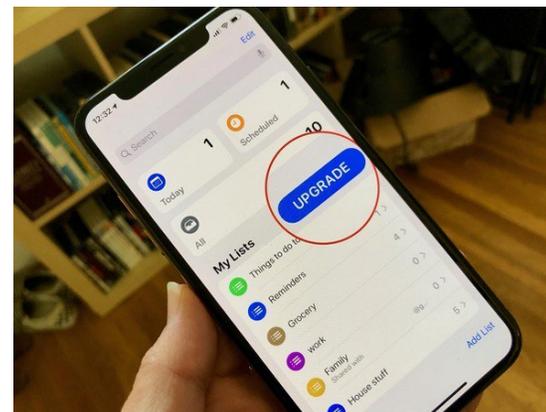
running macOS Catalina, your reminders won't sync across all devices.

Other people you're sharing Reminders lists with will also need to update to iOS 13 if they want to see the changes you've made to a reminder.

The good news is that Apple has provided a way to postpone updating just the Reminders app to the new features.

The first time you open the Reminders app after installing iOS 13, you'll see a notice that some of your devices need to be updated before they can access changes made in Reminders via iCloud. You'll also see a list of the iCloud addresses you share Reminders with that also need to update in order to access any changes you make.

If you don't want to install the iOS 13 Reminders features, just tap "Upgrade Later" to postpone the update. I highly recommend you do this if you use reminders on more than just your iPhone and Apple Watch.



If you choose to upgrade later, you'll see a button next to your "My Lists" section. When you're ready, you can make the switch just by tapping "Upgrade" and following the instructions.

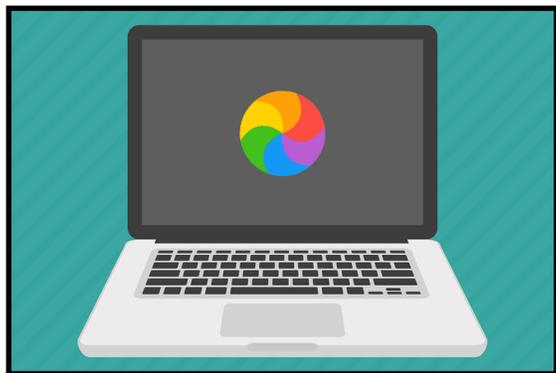
Don't jump the gun on this and make the switch too early. You can't un-upgrade once you've upgraded Reminders to iOS 13.

Tom Nelson posted the following article to *lifewire.com* on January 31, 2019. [bit.ly/2n46OSZ](http://bit.ly/2n46OSZ). © About, Inc. He is a consultant and writer providing Macintosh training, advice, and support. He has written hundreds of articles, tutorials, and product reviews.

## Fix SPOD - How to Fix a Spinning Pinwheel of Death

*Cleaning out the dyld cache can clear a SPOD or beachball*

**By Tom Nelson**



Once in a while, for no apparent reason, you may encounter the SPOD (Spinning Pinwheel of Death). It's that multicolored pinwheel mouse pointer that signifies a temporary delay while your Mac tries to figure something out. In this case, your Mac is trying to think but nothing happens, so the pinwheel keeps spinning, and spinning, and spinning.

Luckily, the SPOD is rarely a sign that your Mac is freezing up. It's more likely that a single application is stalled or frozen. If that's the case, bringing another application to the front or clicking on the desktop will likely bring the Mac back under your control. You can then force quit the offending application.

There's a good chance, though, that the next time you try launching the application that caused the SPOD, you'll end up seeing the spinning pinwheel again.

### Repair Permissions

One of the first things many of us will think of doing is to repair permissions to make sure the application, and any associated files it needs, have the correct permissions required to run. File permissions can get wacky once in a while; repairing permissions is a good general-purpose troubleshooting catch-all.

Repairing permissions was a good first step, provided you're using OS X Yosemite or earlier. With the release of OS X El Capitan, Apple added a new feature that made manually repairing file permissions no longer necessary. Now file permissions are automatically repaired whenever a software update occurs.

As a result, if you're using OS X El Capitan or later, you can skip repairing file permissions and move on to step two.

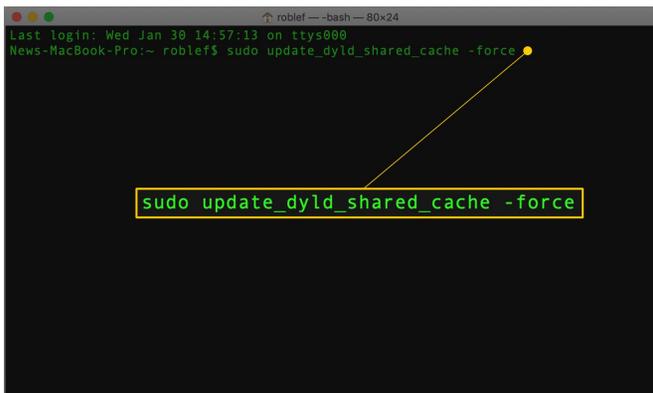
### Dynamic Link Editor

The second thing I do is clear the dynamic link editor (dyld) cache. The dynamic link editor is a way for OS X to load and link programs to shared libraries. If the application in question uses a shared library of routines in OS X (and most applications do indeed use shared libraries), it's the dynamic link editor's job to get the application and the shared library on speaking terms.

The dynamic link editor keeps a cache of recently used library entry points. It's this cache of data that, should it become corrupt, can cause the SPOD. I don't know what causes the cache to go bad, but the phases of the moon and unusual weather patterns are as good a reason as any. The point is that clearing the cache out will usually eliminate the SPOD.

### Clearing the dyld Cache

1. Launch Terminal, located at `/Applications/Utilities/`.



2. At the Terminal prompt, enter the following command.

```
sudo update_dyld_shared_cache -force
```

3. Press Enter or Return.

4. You will be asked for an administrator account password.

5. Once the password is accepted, Terminal may display some warning messages about mismatches in the dlyd cache. Don't worry; these are warnings about the content that is being cleared out and then updated by the command.

6. Clearing the dyld cache can take a few moments. Once it's complete, the normal Terminal prompt will return.

7. You should now be able to use that application without encountering the SPOD.

### Background Processes Can Slow Things Down

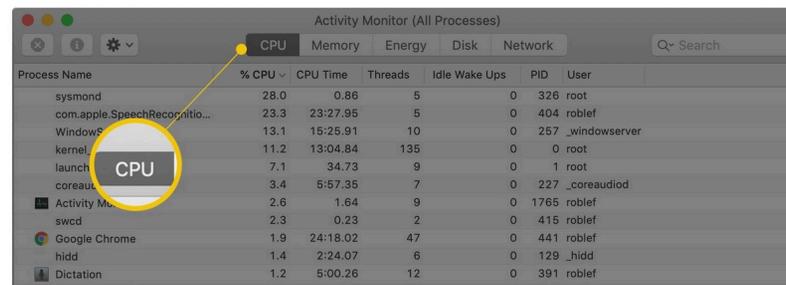
If you still run into the spinning pinwheel, also commonly called the spinning beachball, there are a few more tricks to try.

It's possible the SPOD isn't being caused by the suspected app, but by another app or daemon that may be running in the background. You can usually tell if a specific app, such as Safari, is causing the slowdown by bringing another app to the foreground. If the spinning pinwheel or beachball cursor goes away but returns when you bring the Safari app back to the front,

then it's likely Safari that is having an issue. But if the SPOD continues when you switch to another app, then another app is causing the problem.

This opens up a wide range of possible causes. It could be just about any third-party app that installs a background process that is always running, such as many of the anti-virus apps out there. It could also be one of Apple's own processes, including Spotlight, which can bring a Mac to its knees when it's creating or rebuilding the Spotlight index.

### Spotlight Indexing



You can determine whether Spotlight is the problem by launching Activity Monitor , then:

1. Select the CPU tab.
2. Look for processes with the names "**mds**", "**mdworker**", or "**mdimport**"; these are all part of the MetaData Server process used by the Spotlight app. If any of these have a high percentage of CPU activity (larger than 20%), then it's likely Spotlight is updating its database.

TIP: Use the Search bar in Activity monitor to find all the processes that have "md" in their names.

You can try waiting for the process to end, though it can take a long time if Spotlight is indexing a new drive, a clone you just made, or some other event that has caused a large change in the data storage your Mac has access to.

If you can't wait, you can turn Spotlight indexing off for a specific drive or folder by following the directions in the Using Spotlight's Preference Pane to Customize Search guide. Remember, when you turn Spotlight indexing back on for the selected drive or folder, the indexing will start from the beginning.

---

*Stanley Goodner posted the following article to lifewire.com on June 24, 2019. [bit.ly/2IjPWPu](http://bit.ly/2IjPWPu). © About.Inc. He has spent over a decade writing tech-oriented articles and product reviews. He has a B.S. in Electronics Engineering Technology.*

## How to Save Old Photos to Your Computer

*Four ways to digitize photos so you can keep them forever*



*Digitizing old photos is a great way to preserve those memories.*

**By Stanley Goodner**

Whether you've chosen to dabble in photography using a 35mm film camera, or have uncovered an old box filled with [pictures](#) from decades ago, you might be wondering how to save photo prints and negatives to your computer. The good news is that there are several options, depending on how much involvement is preferred. You can digitize and archive photos by using:

- Photo scanners

- Digital cameras (or smartphone/tablet)

- Retail stores

- Online services

Once you have the digital photo files uploaded to a computer, it's easy to [copy to another folder](#), print, share to social media or [image hosting sites](#), save to [local backup](#), save to [personal cloud storage service](#), and/or save by using an [online backup system](#). You spent the time taking and preserving all of these memories; the backups help ensure that copies will always be there in the future for those who want to see them. And with some practice, you can edit and cleanup photos and have new prints made. Photo Scanner

The photo scanner remains one of the most popular ways of digitizing photo prints and images. All it requires is hardware (you'll want a [quality document/photo scanner](#)), a computer or laptop, and ample time to process and save the pictures. It can be done in the convenience of your own home—or anywhere with a portable scanner. You often have the option to retouch images before performing final saves. If you don't yet own one, there are [considerations when choosing a photo scanner](#). Some are slim and compact, while others are bigger due to having both a flatbed and a document feeder for scanning. Some come with adapters that let you scan negatives, transparencies, and slides, while others do not. Scanners also have hardware specifications capable of varying levels of [resolution and color depth](#). Although photo scanners typically come pre-packaged with their own scanning program, you can use most any image editing software

(e.g. Photoshop, free alternatives to Photoshop) that lets you import photos through a connected scanner. For the best possible accuracy while scanning, be sure to first:

[Calibrate your PC/laptop monitor](#)

[Calibrate your scanner](#)

Carefully clean photos and the scanning surface

That last step is very important. Any smudges, fingerprints, lint, hair, or dust particles left on photos or the scanning surface will show up in the digitized image. Soft microfiber cloths and cans of compressed air are useful for safe cleaning. Once that's done, you're all set to [create and edit digital photos from scanning physical prints](#). The downside of this method is that it can be a time-consuming process to scan, edit, name, save, and organize all of the photo files. But at least you have full control without having to spend a dime.

### **Digital Camera (or Smartphone/Tablet)**

For the do-it-yourself approach, a photo scanner delivers the most high quality and consistent results. However, digital cameras — and even smartphones and tablets with high megapixels — can work in a pinch to scan photos. Although most digital [mirrorless and DSLR cameras](#) have a variety of [scene modes](#) to choose from to best match shooting situations, some advance preparation will be required on your part.

When [using your digital camera as a scanner](#), you'll need to pay extra careful attention to a few aspects.

**Lighting:** Ambient light should be as even across a photo's surface as possible with minimal (if any) glare and no shadows. The temperature of the light source is also important for accurate color reproduction; many digital cameras can automatically compensate (white-adjust) for this.

**Stability:** If you want to create an archive-quality copy of a photo with a digital camera, don't assume you can do it by hand. The slightest body movement can throw off focus and perspective—

foreshortening is what happens when the reproduced image looks like a trapezoid instead of a rectangle with perfectly squared corners. A tripod will help guarantee that the camera lens stays parallel to photos, and using the self-timer function (a remote shutter can also work) will eliminate shake.

**Quality:** Be sure to double check your camera settings so that it's set to the highest/superfine resolution (when in doubt, [shoot in RAW](#)), lowest ISO, and moderate/high aperture (f/5.6 or more). You can bracket your shots (i.e. one normal exposure, one at a higher f.stop, one at a lower f.stop) for each photo, since it's easier to judge exposure on computer monitors than camera LCD screens.

As long as imperfection isn't a big deal — archive copies can always be created later on — you can turn a smartphone or [tablet into a scanner](#). Some camera and/or image editing apps offer white balance adjustment, auto color correction, foreshortening compensation, and a host of other helpful tools. Others, such as [PhotoScan by Google Photos](#) (available for [Android](#) and iOS), are specifically designed to create and enhance digital photo scans from mobile devices.

To transfer photos from a digital camera or smartphone/tablet to a computer, you can either use the product's data/sync cable or a separate memory card reader. Once a device/card has been connected, simply navigate to the [DCIM folder](#) and [copy all the files to your computer](#).

### **Retail Store**

If you don't have a photo scanner and aren't interested in using a camera/smartphone to digitize photo prints, you can always visit a local retail store. Places such as Walmart, FedEx, Staples, Walgreens, Costco, Office Depot, Target, CVS, and others offer photo scanning kiosks and/or drop-off services. Prices, quality of scans, turnaround time, and the amount of help you get from store associates (i.e. if you're not very familiar with scanners/kiosks) can vary.

When it comes to developing film/negatives, be sure to ask about the details first. While many of the aforementioned companies can process prints and digitize images, some *won't return your original film/negatives*.

Scanned photos from retail stores typically come on a CD, DVD, or flash drive. In order to upload photos to the computer, place the CD/DVD into the [optical disc drive](#); flash drives plug into an open USB port. Navigate to where the files are stored on the media and then [copy them to the desired folder on your computer](#). You can put the physical CD/DVD or flash drive in a safe place as an extra backup.

### Online Service

The alternative to visiting your local retail store (and from doing it yourself) is an [online photo scanning service](#). You can find hundreds of these types of sites, all with varying prices, shipping requirements, quality, turnaround time, enhancements/specialities, etc. If you want to guarantee the best results, particularly if you have old and/or damaged photo prints in need of digital restoration, online services will far exceed what you would get from a retail store. Although online services tend to cost more than your local retail, you can expect a higher-overall quality of scans that won't disappoint.

Our recommendations:

- Best all-around service: [MemoriesRenewed.com](#)
  - Best for serious retouching and restoration: [Dijifi.com](#)
  - Also good: [DigMyPics.com](#) and [ScanMyPhotos.com](#)
- 

*William Harrel posted the following article to lifewire.com on June 27, 2019. [bit.ly/2oVosZE](https://bit.ly/2oVosZE). © About.Inc. He has been writing about computer technology for over 30 years. He has authored or coauthored over 20 books,*

## How to Choose a Photo Scanner

*Photo scanners can be very simple or ultra-complicated — you choose*



### By William Harrel

You'd think that as long as [digital cameras](#) and, more importantly, photo scanners, have been around, nearly all the photos in the world should already be digitized. Alas, apparently, we're still not even close, or maybe new hard copy prints get generated every day — perhaps both. In any case, the point is that, just as the need for photo [printers](#) continues, so does the need for photo scanners. However, not all photo scanners are the same, and it really depends on what you plan to scan, the required scan quality, and how often you plan to scan photographs, to determine how sophisticated a machine you need.

## About Photo Scanners

The best photo scanners are, of course, drum scanners, but only specialized imaging service bureaus can afford those. The next best are high-resolution flatbed scanners, such as Epson's Perfection V850 Pro Photo Scanner. Not only does it scan at ultra-high resolutions, but it also comes with a set of adapters for scanning transparencies, slides, film, and negatives, as well as fairly decent photo enhancing and correction software.

If you want to use your scans of photos, transparencies, slides, and such in print layouts or other applications that require ultra-high resolutions, you'll need to scan them at high-enough resolutions, or dots per inch (dpi), that they can be enlarged without decreasing image quality. Good photo scanners, such as the Epson model listed above, for instance, can scan as high as 6,400dpi and beyond.

For example, to convert a slide to an 8x10-inch image, you need to scan at about 2,000dpi or higher.

And the pixels per inch (ppi) for an image with the physical dimensions of 8x10 inches is 1,800x3,000, at 600dpi.

## Shopping Around

So you've already looked around and you found a flatbed scanner like the one described in the previous section — for only \$100. It scans at 9,600dpi, has a 48-bit color bit depth, and it comes with all the image-editing and other software required to touch-up and save the images you scan, as well as [optical character recognition software \(OCR\)](#), and document cataloging software.

A great deal, right? Well, yes, if all you're doing is scanning images for Facebook and other social media sites, this setup is fine. But keep in mind that much of the resolution and color reproduction achieved in the less-expensive model are the results of interpolation and other software routines, or a lot of smoke and mirrors, whereas the high resolutions and [color](#)

[depths](#) captured by the \$1,000-scanner (or higher) are actually picked up and digitized by the lenses inside the scanner. In other words, you get a detailed dot-per-dot reproduction, rather than an image where the scanner (and accompanying interface software) compensate for a lack of high-quality, high-res sensors.

## Taking the Plunge

So which photo scanner will work for you? Truthfully, if the majority of your images will as mentioned, show up on the web, or perhaps saved in your digital catalog either on your computing device or your favorite cloud site, the \$100 scanner will probably work just fine for you. Only professionals who intend to print or use some other high-resolution version of the images somewhere else, require the treatment performed by a [high-end photo scanner](#). And yes, sometimes, depending on your application, that scanner atop of your multifunction printer will do just fine — sometimes.

---

Scott Orgera posted the following article to [lifewire.com](http://lifewire.com) on August 21, 2019. [bit.ly/2mw3vU6](http://bit.ly/2mw3vU6). © About, Inc. He has been as a programmer, quality assurance lead, and writer for 25 years.

## The 7 Best Free Photoshop Alternatives

*You don't need Photoshop to edit photos like a pro*



### By Scott Orgera

First released roughly three decades ago, Adobe Photoshop is the gold standard preferred by some of the world's top visual artists. Its powerful tools help photographers create almost anything the imagination conjures.

Photoshop is now licensed as part of the Adobe Creative Cloud suite of subscription-based software. But instead of paying the monthly fee if your budget is constrained or your use case is minimal, try a free, open-source alternative.

Tip: Before you download a Photoshop alternative, plan for your specific needs. For example, not all free Photoshop alternatives support the Adobe application's default [PSD format](#). Others, meanwhile, will not be able to

recognize some multi-layered Photoshop files. If you need a key Photoshop feature, you'll find it easier to narrow your search list if you filter based on features.

## GIMP

### What We Like

- Constantly updated with new features.
- Highly customizable and extensible.

### What We Don't Like

- Limited support for layers, macros, and custom shapes.
- Cluttered UI with annoying floating windows.

One of the most full-featured Photoshop alternatives, GIMP (short for GNU Image Manipulation Program) offers such a large set of features that even the most complex tasks can be achieved without any strain on your budget. They say that you get what you pay for, but in GIMP's case, that idiom doesn't necessarily ring true. With a very active [developer community](#) that has historically listened to user requests and feedback, this free option continues to advance as raster editor technology expands.

While not always as intuitive as Photoshop in terms of functionality and design, GIMP makes up for some of its perceived clumsiness with several [in-depth tutorials](#) for both beginning and advanced users that help you use the majority of its components with little or no pre-existing knowledge of the open-source application. With that said, if you're only looking for the very basics in a raster-based graphics editor then GIMP may actually be a little too much and you may benefit from one of the simpler alternatives on our list.

Available in almost twenty languages for the Linux, Mac, and Windows platforms, GIMP recognizes almost all file formats that you'd expect from a paid editor like Photoshop including [GIF](#),

[JPEG](#), [PNG](#) and [TIFF](#) among others, as well as partial support for PSD files (not all layers may be readable).

Also similar to Photoshop, a large number of external plugins are available that enhance GIMP's functionality further. As always, download at your own risk when dealing with non-native repositories.

## Pixlr

### What We Like

- Extensive layer support with multiple blending modes.
- Includes built-in filters and adjustment tools.

### What We Don't Like

- No social media integration.
- Layer masks tool is cumbersome to use at first.

A browser-based alternative to Photoshop, Pixlr is owned by well-known software developers Autodesk and is quite robust when it comes to available features and allows for progressive editing and enhancing as well as original image design.

The Pixlr Express and Pixlr Editor web apps will run in most modern browsers as long as you have [Flash](#) 10 or above installed; they offer a significant number of integrated filters along with limited layer support. Pixlr recognizes the main graphical file formats such as JPEG, GIF, and PNG and also allows you to view some PSD files, although those larger in size or complex in nature may not open.

The web-based Pixlr even has a handy Webcam feature built right into its dashboard that lets you capture and manipulate photos on-the-fly.

In addition to the browser version, Pixlr also has free apps for both [Android](#) and [iOS](#) devices that let you perform a number of editing features from your smartphone or tablet. The Android app

is so popular, in fact, that it has been installed on well over 50 million devices.

## Paint.NET

### What We Like

- Streamlined interface is a breeze to navigate.
- Helpful keyboard shortcuts.

### What We Don't Like

- UI lacks a tool for managing plug-ins.
- Text can't be edited after it's deselected.

A free Photoshop alternative strictly for Windows versions 7 through 10, the Paint.NET interface is reminiscent of the operating system's Paint application; the built-in image editing tool for PC users worldwide. The similarities are no coincidence, as the original developer's intent was to replace MS Paint with something a little better.

That was a long time ago, and Paint.NET has since grown by leaps and bounds to the point where it's comparable in some ways to the more advanced editing software on the market, both free and paid. This includes the ability to use multiple layers and blending, all the while maintaining a fairly simple interface that lends itself to even the most novice user. If you do get stuck, the Paint.NET forums are an invaluable source for assistance where inquiries are sometimes answered in mere minutes. Couple that with the tutorials found on the same website and this Windows-only graphics editor offers a user-friendly experience.

Although Paint.NET does not provide some of the higher-end functionality of Photoshop or even GIMP, its feature set can be expanded upon through the use of external plugins. For example, the application does not natively support PSD files but can open Photoshop Documents after the PSD plugin is installed.

The self-proclaimed fastest image editor available, Paint.NET can run in almost two dozen languages and is free to use for both business and commercial use with no restrictions.

## PicMonkey

### What We Like

- Supports cloud storage integration.
- You can make custom collages without signing up.

### What We Don't Like

- No layer support.
- Free version is rather limited.

Another platform-independent, web-based design and editing tool with a lot to offer is PicMonkey, which was seemingly designed with the neophyte user in mind but also packs a punch for those looking for more state-of-the-art features. As long as you have a browser running Flash, PicMonkey is accessible on virtually any platform and lets you start your creation from scratch or begin editing an existing image file in under a minute.

PicMonkey will not replace Photoshop's more advanced functionality and you won't have much luck with PSD files, but it is ideal for working with filters and even creating collages from within your favorite browser. The free version offers quite a bit in terms of features, but you'll need to pony up some cash if you want access to some of the app's exclusive effects, fonts, and tools as well as an advertisement-free experience.

The premium adaptation of PicMonkey features a seven-day free trial that can be activated by providing your email address and payment information. If you want to continue using its advanced functionality long-term, though, a monthly fee of \$7.99 or \$47.88 for an annual membership is required.

With an oft-updated blog featuring a bevy of tips and tutorials, you should be able to figure out whether or not PicMonkey is the right option to suit your needs within the week-long trial period.

Smartphone and tablet users may also want to try the free PicMonkey Photo Editor app, available for both Android and iOS platforms.

## SumoPaint

### What We Like

- Great layer support.
- Affordable pro package.

### What We Don't Like

- Won't open newer file formats.

One of our personal favorites, SumoPaint's interface will look familiar if you have past Photoshop experience. The similarities are more than just skin deep, too, as its layering functionality and fairly wide range of editing tools, including several brushes and wand types, make it a formidable alternative.

The free version of SumoPaint runs in most Flash-enabled browsers and is mainly supported by on-page ads. There is also a Chrome Web App available for [Chromebooks](#) as well as users running Google's browser on other desktop operating systems.

More intricate projects may not be suitable for SumoPaint, and its file support is somewhat limited and does not include Photoshop's default PSD format. You can open files with traditional image extensions such as GIF, JPEG, and PNG while edits can be saved in the app's native SUMO format as well as JPEG or PNG.

If you try the free version and feel that SumoPaint is what you've been looking for, then you may want to give Sumo Pro a whirl. The paid version allows for an ad-free experience as well as access to additional features and tools for about \$4 per month if

you pay for a year in advance. Sumo Pro also offers a downloadable version of its software that can be used while offline, as well as access to a dedicated technical support team and cloud storage.

## Krita

### What We Like

- Customizable interface.
- Brush tools feature detailed previews.

### What We Don't Like

- Updates are often unstable.
- Consumes a lot of CPU resources.

An interesting editing and painting tool, Krita is an open source application that has seen its feature set expand significantly in recent years. With a nifty palette and a seemingly endless amount of brush customizations that can be stabilized to smooth out even the most unsteady hand, this Photoshop alternative supports most PSD files and offers advanced layer management.

Free to download, the regularly updated desktop application also uses OpenGL and allows you to author and manipulate [HDR images](#) — among many other benefits. Available for Linux, Mac, and Windows, Krita boasts a fairly active forum containing sample artwork created by members of its user community.

There is another version of Krita optimized for ultrabooks and other touchscreen PCs, named Gemini, available from Valve's Steam platform.

## Adobe Photoshop Express

### What We Like

- No registration required.
- Excellent white balance adjustment with numerous presets.

### What We Don't Like

- Requires an internet connection to use.
- Only edits JPEG files.

While Adobe charges a fee to use its main Photoshop software, the company does offer free image editing tools in the form of the Photoshop Express application. Available for Android, iOS and Windows tablets and phones, this surprisingly capable app allows you to enhance and tweak your photos in a number of ways.

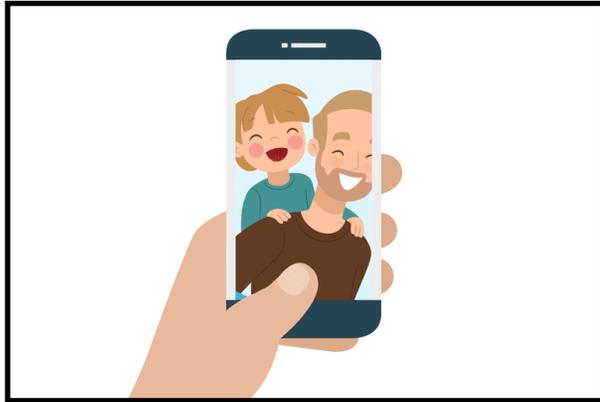
In addition to correcting problems such as red eye with just a tap of the finger, Photoshop Express also makes it easy to apply unique effects and incorporate custom frames and borders before sharing your pictures on social media or elsewhere from right within the app itself.



Tim Fisher posted the following article to about.com on September 04, 2019. [bit.ly/2o5ABL3](http://bit.ly/2o5ABL3). © About.com. He is a freelance technology author, co-owner of a technology services company for small businesses, and author of *Windows 8 Basics in 30 Minutes*.

## The 5 Best Photo Editor Apps of 2019

*Paid or free, Apple or Android, these are the best!*



### By Tim Fisher

Photo editing should come easy on our [phones](#) and [tablets](#) because, after all, that's what most of us use to take pictures every day. There are tons of image editors for [iPhone](#) and [Android](#) alike, most with similar features but some with very unique capabilities.

If you want to make a picture black and white or crop out the edges, you can probably stick with the default photo editor built-in to your phone. However, sometimes you need or want to do more, like overlay one image on top of another, apply unique filters, make certain colors pop out, add stickers or text, choose from dozens of picture frames, etc.

Some image editor [apps](#) aren't free but most are, and even the paid ones usually have a free, feature or time-restricted lite

version. Whether you're looking for an Android photo editor or one for you iPhone or [iPad](#), you can find all the best editors in this list.

### 1 [Pixlr](#)

#### What We Like

- Lots of useful tools
- One-tap fix-it buttons
- Adjust the strength of almost every tool
- Tools can be favorited for quicker access later
- Save to PNG or JPG

#### What We Don't Like

- Isn't completely ad free
- Effects aren't as fluid as some apps

One great photo editor app is Pixlr. It's free, has minimal ads, and includes lot of cool features.

One feature that stands out is that with each edit, you can press your finger down on a "before" button to see what the image looked like just before you applied that effect, which is great for deciding if you should commit to it or not.

You can share your edited image on social media as well as save it back to your phone or tablet in various sizes like small, medium, max, or a custom size.

Some of the tools included in this free photo editor app include the standard ones like crop and rotate, but it also has an autofix, adjustment, blur, splash, smooth, sharpen, red eye, double exposure, and spot healing brush tool.

Pixlr has a set of brush tools you can use to paint various things on the image. There's one for brightness, darken, and pixelate. They're extremely useful versus an image-wide option because

instead of darkening the whole image, for example, you can apply darkened spots to specific problem areas. There's also a regular doodle tool.

We really love the one-tap effect and styles you can apply to pictures with Pixlr. You can pick from options like a pencil, sketch, poster, cross, watercolor, polly, and other styles. There are lots and lots of effects, too, in categories like atomic, creative, unicolor, vintage, too old, subtle, and soft. In the same area of the app are overlays so that you can quickly drop a burn effect right over the picture, or an effect like bubble, glitter, glaze, metal, etc.

What makes Pixlr vastly different than some photo editor apps is that you get to really customize the level that an effect can take on your photo. For example, if you pick a *glaze* overlay to apply to your image, you can use the scroll bar to lessen how much of the effect is actually seen once applied, or the eraser tool to remove the effect on only parts of the image. You can do this to multiple effects, overlays, and styles to really personalize it how you wish.

The Pixlr app also has lots of borders and stickers that, again, are just one tap away. The text tool lets you change the font type to one of several options and can be any color you want. The opacity can be adjusted for all of those things as well.

This app does show ads sometimes, like when you're about to save your picture, but they're not intrusive at all. There's a good chance you'll glance right over them.

Probably the biggest issue with this photo editor is that when you're choosing how much of an effect to apply, by sliding the scroll wheel left or right, you can't see how the effect looks until you lift your finger. Most other apps show the result in real time but, unfortunately, Pixlr does not.

This photo editor is free for Android and iOS.

## 2 Snapseed

### What We Like

- Free with no ads
- Really simple to use
- Edit RAW files
- Precise control over how much of a tool is applied
- Save a copy with the ability to undo edits later

### What We Don't Like

- Filters and other tools are mashed into one menu

Snapseed is a free photo editor app from Google. It's really simple at first glance but does include quite a bit of editing tools.

Instead of using a scroll tool to increase or decrease the intensity or strength of effects and other tools, this app has you slide your finger to the left or right of the screen to see the changes in real time.

Another big feature not found in most photo editor apps is the **View edits** option in Snapseed. This lets you view a list of all the edits you've made since the beginning, and lets you jump back to a specific point in one tap. It's like the version history you might be used to in your online documents but with image edits. This definitely beats hitting an undo button a dozen times, and you can even save the picture and reopen it later to undo changes.

When you first open Snapseed, unlike other apps that often have lots of buttons, there's just a **LOOKS**, **TOOLS**, and **EXPORT** button. The first two, of course, are where you'll find the editing options and the last one is for sharing and saving the image. There's also a small **Settings** menu for adjusting the sizing, format, and quality of exports—you can save a [PNG](#) or a [JPG](#) with custom compression.

In the first menu is a list of one-touch effects you can apply to your image that will apply preset effects automatically. Some of them are called Last Edits, Portrait, Smooth, Pop, Faded Glow, Morning, Bright, Fine Art, and Silhouette. Tap one to instantly apply it to the picture. Once you commit to one, you can go back and apply another on top of it, which is something many photo editors won't let you do.

Or, if you want precise control over how the tools are used, use the **TOOLS** menu. Many of them are common and can be found in other photo editor apps but some are entirely unique to Snapseed. Filters and editing tools are combined into one screen.

For example, there's a crop, rotate, perspective, and expand option but also a curves, white balance, selective brightness, exposure and dodge/burn brush, glamour glow, head pose, lens blur, HDR scape, and other fun tools.

Snapseed is also a great app for applying frames and text to a photo. There are over 20 frames to choose from and several meme-like text options.

You can get Snapseed free for iPad, iPhone, and Android [devices](#).

### 3 **Enlight**

#### What We Like

- Advanced yet not hard to use
- Apply effects to specific areas only
- Includes basic tools, too
- Export to TIFF, PNG, or JPG with varying file sizes

#### What We Don't Like

- Isn't free
- Could be overwhelming with all the options

The Enlight photo editor is pretty amazing. You can think of it like the Photoshop of image editors, but for your iPhone or iPad (it's actually better than the [mobile Photoshop app](#) in our opinion). It has all those normal editing tools you hope to have in an app but is also really useful for putting creative spins on your images.

If you're willing to trade just a few bucks, you'll have quite a robust image editor in your hands at all times, one they call "every photo app you've ever needed, wanted, or dreamed of" combined into this one app.

This photo editor app is definitely a bit more advanced than the others listed above, but don't let that come off as a bad thing. While some apps loaded with features are difficult to use because of poor design, Enlight uses pop-out menus for organization and has tutorials for help understanding all the features—just pull down from the top of the screen for info about any tool.

Enlight can flip, rotate, skew, and straighten images. A similar feature that makes this app stand out from others, especially free ones, is its *Refit* tool. Select the parts of the image that should remain in the photo, and if the background is simple enough, refitting will move those parts together to crop the photo without affecting those objects. It's very neat!

Another thing that makes Enlight so different than most free photo editors is its selective editing tool called *Target*. Use it to apply color, exposure, contrast, sharpness, and clarity to particular parts of an image instead of the whole canvas. This is really useful since some photos don't need a blanket edit.

Enlight is also known for its filters, separated into categories like *Analog*, *BW*, and *Duo*. Pick a category, choose a filter, and use your finger or [stylus](#) to control how strong the preset should appear on your image, by swiping to the left or the right. The *Duo* section is particularly interesting because it lets you tint the image with a blend of two colors, with custom overlap options.

There are also artistic tools in Enlight so you can convert your photos into paintings or drawings. Much like the other options in this photo editor, you can provide as much control over the effect as you like to make it only partially sketched, for example, or provide a full painted look.

One more thing worth noting about the Enlight photo editor app is the *Mixer* tool that lets you create a double exposure effect to combine two images together, forming a hybrid photo like you see in the image above. It's a bit like [Union](#) and similar apps but better since you can edit in Enlight and stay there for double exposure, too.

This app is for iOS only, and costs \$3.99 USD.

The same creators of this app, Lightricks, have a free app called [Enlight Photofox](#), but it has different features.

## 4 PhotoGrid

### What We Like

- Lots of unique features
- Most of the tools are free to use
- Very easy to use

### What We Don't Like

- Saves with a small "PHOTOGRID" watermark
- Has ads

PhotoGrid is a different kind of photo editor app. Instead of providing just editing tools, you can use it to make a photo or video collage, scrapbook, [GIF](#) or still meme, slideshow, poster, filmstrip, and more.

This free image editor app also works as an [augmented reality](#) camera, letting you overlay stickers and hats and other things directly onto your face in real time.

Plus, you can follow other PhotoGrid users and keep tabs on what they post in the *Feeds* section of your app.

PhotoGrid is on an entirely different level than the other image editors in this list. While it does have normal editing capabilities, it doesn't seem built for that, and honestly that's probably not why most people use this app.

On the main screen of the app are all your options. You can pick any of these: Grid, Edit, WowCam, Video, Retouch, Big Head, Scrapbook, Meme, Slide Show, Filmstrip, Poster, Pattern Venus Filter, Twinkle, and Instant Share.

These tools let you do things like combine videos and images into collages, take videos or image selfies with live stickers, build GIF memes, make new wallpapers for your phone, build stylish posters, make your head look like a balloon, and, of course, typical editing where you can add text, draw on the image, crop or rotate the photo, adjust skin tone, blur, and add a border.

This app clearly has a lot built-in to it, but at the same time it lets you customize a lot of what you do. For example, when making a collage with PhotoGrid you can adjust each individual image in its frame and combine other tools to round the edges, add text, import stickers, apply filters, and more. Sometimes, you can even adjust the intensity or opacity of a tool.

PhotoGrid is free for Android and iOS. If you want more features, you can watch ads to get something for free, otherwise you can pay (usually around \$1) to get things like more poster templates, backgrounds, stickers, etc.

## 5 PicsArt Photo Studio & Collage

### What We Like

- Advanced for a free app
- Millions of free stickers
- Supports layers in some tools
- Lots of one-touch effects

- Save to your PicsArt account

### What We Don't Like

- Must log in to edit photos
- Many of the filters and other options are only free during a 3-day trial
- Lots of ads, both sectional and fullscreen

PicsArt Photo Studio & Collage is different from these other photo editors in a number of ways, but the most notable is that when you're editing a portrait, there are various tools that can automatically recognize where the person is located and isolate it from the rest of the picture to make editing a lot easier than manually tracing out the background.

Some photo editors let you adjust the strength of some of the tools, like filters, so that only part of it bleeds through to the photo. While this isn't possible with the PicsArt app, it does have an eraser tool that can remove a filter for select areas of the photo, plus an even more impressive button that will identify a face/body and immediately remove the filter from that area.

Tons of other advanced editing tools are included, too, like a crop, dispersion, clone, stretch, motion, perspective, curves, and shape crop tool.

Images can be shared with friends through the app via *Remix Chat*. Plus, every user has a profile page friends can visit to see what they've been sharing with the community.

You can take part in what the app calls *Challenges* to remix certain images and possibly win prizes. For example, one might be a picture of a woman with a bare arm where you have to [apply a tattoo](#).

In addition to all the stickers made by other members that you can freely use as often as you like, there are also free images accessible from inside the app.

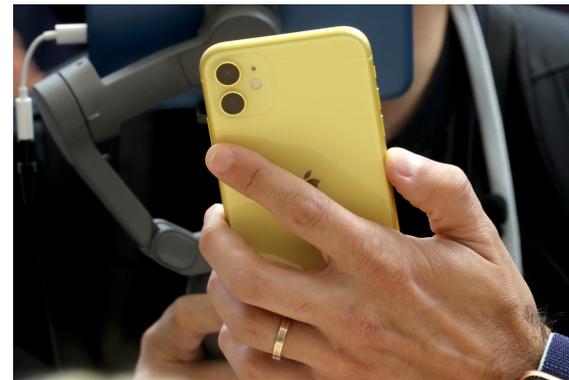
This free [photo editor](#) runs on iOS, Android, and [Windows 10](#).

Brian X. Chen posted the following article to nytimes.com on September 19, 2019. [nyti.ms/2mEgbsH](https://nyti.ms/2mEgbsH). © The New York Times Company. He is the lead consumer technology reporter at The New York Times, and has been a technology commentator on a number of radio and television programs.

---

## iPhone 11 and 11 Pro Review: Thinking Differently in the Golden Age of Smartphones

*This is not your typical gadget review. That's because it is time to rethink when to upgrade your iPhone.*



*Now is the moment to ask: Do we really need to upgrade our iPhones every two years?*

### By Brian X. Chen

Over more than a decade of writing about technology, reviewing a new iPhone has long been one of my simplest assignments.

Year after year, the formula was this: I tested the most important new features of Apple's latest smartphone and assessed whether they were useful. Assuming the newest iPhone worked well, I

generally recommended upgrading if you had owned your existing smartphone for two years.

But with this review of the [iPhone 11, 11 Pro and 11 Pro Max](#) — which Apple unveiled last week and will become available Friday — I'm encouraging a different approach. The bottom line? It's time to reset our upgrade criteria.

That's because we are now living in the golden age of smartphones, when the gadgets' improvements each year are far from seismic. Devices that debuted three years ago remain zippy and more than capable. Those with the iPhone 7 from 2016, for example, still have a very good phone with a stellar camera and fast speeds.

So now is the moment to ask: Do we really need to upgrade our iPhones every two years?

Based on my tests of the iPhone 11, 11 Pro and 11 Pro Max, the answer is no. Don't get me wrong: The newest models are nice. Apple has made them speedier, improved the cameras and lengthened their battery life. The new lineup also starts at a lower price of \$700, down from \$750 a year ago, which is a relief in an era of skyrocketing smartphone costs.

But none of this is enough to warrant an immediate upgrade if you have had your smartphone for only two years. The latest iPhones just aren't a big leap forward from [last year's iPhones](#) or even the [iPhone X](#) from 2017.

So here's what I ultimately suggest: You should definitely upgrade if your current device is at least five years old. The iPhone 11 models are all a significant step up from those introduced in 2014. But for everyone else with smartphones from 2015 or later, there is no rush to buy. Instead, there is more mileage and value to be had out of the excellent smartphone you already own.

## Comparing the iPhones 11s with the iPhone X



*Apple iPhone 11 Pro*

I tested the new iPhones for a week, starting with the \$700 entry-level iPhone 11 with a 6.1-inch display, which I used as my primary phone for three days. Then I switched to the iPhone 11 Pro, the \$1,000 model with a 5.8-inch screen, for two days. And then finally the iPhone 11 Pro Max, the \$1,100 model with a jumbo 6.5-inch screen, for another two days.

Then I compared the results with my notes and photos from testing the iPhone X in 2017. What I found was that the iPhone 11 was better, but not profoundly so.

### **Here were the notable differences between the iPhone 11s and the iPhone X:**

- All the iPhone 11 models have a new ultra-wide-angle lens in their cameras, which provides a wider field of view than traditional phone cameras. This makes them handy for shooting landscapes or large group gatherings. The iPhone X lacks the ultra-wide-angle lens, but its dual-lens camera is capable of shooting portrait-mode photos, which puts the picture's main subject in sharp focus while softly blurring the background.

- The newest iPhones all have the same computing processor, A13 Bionic, which is about 50 percent faster than the iPhone X. While that may sound significant, the iPhone X is already incredibly fast at shooting photos and running apps and games.
- The new iPhones all have longer battery life. Even after a day of heavy use, which included taking phone calls, using maps and shooting lots of photos, each iPhone had lots of juice remaining — at least 30 percent — by bedtime. After similar tests with an iPhone X two years ago, the battery had about 15 percent left by bedtime.
- The back of the Pro models is composed of a rugged glass that makes them scratch-resistant. This is impressive, but if you're spending \$1,000 on a phone, you will probably protect it with a case that covers the back anyway — just as many iPhone X owners do.
- The Pro models have OLED displays that are slightly brighter than the screen on the iPhone X.

There are lots of little things that are somewhat better on the new iPhones than on the two-year-old iPhone X. For early adopters who are keen to have the latest and greatest tech, those differences may add up to a substantial upgrade.

But for most of us, the upgrades won't meaningfully change our phone experience.

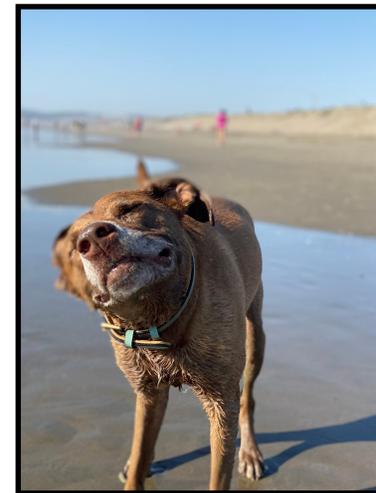
### Contrasting the phone cameras

The most noteworthy new feature on the iPhones 11s is the ultra-wide-angle lens. Using the ultrawide mode is simple and seamless: You pinch outward to zoom all the way out. On a beach, the wider view captured my dogs playing on the sand, the ocean waves and the adjacent highway.



*The ultra-wide-angle lens on the new iPhones takes photos with a wider field of view than traditional cameras.*

The telephoto lens on the iPhone 11 Pro did an exceptional job zooming in on my dog Mochi's snout as she shook some water off her head.



*The telephoto lens on the Pro models can zoom in closely without losing much detail.*

The new iPhones also have a new mode for shooting photos in low light. Once the camera detects that a setting is very dark, it automatically captures multiple pictures and then fuses them together while making adjustments to colors and contrast. The result was that photos taken in low light without flash look brighter, in a natural way.



*The new iPhones include a low-light mode, which captures multiple images at different exposures and fuses them into one, to make a picture look brighter.*

Photos taken with the iPhone 11 and 11 Pro looked crisp and clear, and their colors were accurate. But after I finished these tests, I looked back at my archived photos taken with an iPhone X.

Those pictures, especially the ones shot with portrait mode, still looked impressive. Some of the low-light ones looked crummy in comparison with the ones taken by the iPhone 11s, but I wouldn't recommend that you buy a new phone just to get better night photos. You could always just use flash.

## When should I upgrade then?

Each year, the most common question I get from friends and colleagues is whether they should buy a new iPhone. So here's a list of considerations in any decision about upgrading.

The simplest place to start is software. Apple's newest mobile operating system, [iOS 13](#), will work only on iPhones from 2015 (the iPhone 6S) and later. So if you have an iPhone that is older than that, it is worth upgrading because once you can no longer update the operating system, some of your apps may stop working properly.

For those with younger iPhones, there are ways to get more mileage out of your current device. While the newest iPhones have superb battery life — several hours longer than the last generation — a fresh battery in your existing gadget [costs only \\$50 to \\$70](#) and will greatly extend its life.

If you have the iPhone 6S from 2015 and the iPhone 7 from 2016, the iPhone 11s are speedier, with camera improvements and bigger displays. That makes an upgrade nice to have but not a must-have.

But if you spent \$1,000 on an iPhone X two years ago, then hold off. The iPhone 11s just aren't enough of an innovation leap to warrant \$700-plus on a new smartphone.

If you wait another year or two, you will most likely be rewarded with that jump forward. That might be an iPhone that works with fast 5G cellular networks, or a smartphone that can wirelessly charge an Apple Watch.

Patience has its benefits — and so will breaking free of the iPhone's automatic two-year upgrade cycle.

---

Elise Moreau posted the following article to *lifewire.com* on September 4, 2019. [bit.ly/2mJ3cWg](https://bit.ly/2mJ3cWg). © About.Inc. She is a professional blog writer, copywriter, and digital marketing consultant for businesses and entrepreneurs.

## 4 Search Tools to Find Email Addresses

*These tools can help you find almost anyone's email address*



### By Elise Moreau

People protect their email addresses for good reason and even if you try to run an [email address search](#) by Googling somebody's full name with the word "email," you're often unlikely to find anything. Putting it right out there in plain sight on the web invites anyone and everyone to contact them—even spammers.

But in the age of social media, is email still really relevant? Should we all just give up on trying to find people's email addresses and resort to Facebook Messages and Twitter Direct Messages instead?

Nope. At least not yet. Emailing someone can still be more powerful than contacting them on social media.

Not only is it the most personal and professional way to make contact, but it might also be the best way to reach someone quickly (not everyone checks their Facebook Messages or Twitter DMs daily). Plus, *everyone* has an email address.

If you would like to shoot an email to someone but don't know how to contact them, take a look at some of the very best tools that can help you find somebody's email address in as little as a few seconds.

### 1 Use Hunter to Search for Email Addresses by Domain

#### What We Like

- You don't need to know the person's name.
- Shows sources where the email address was found.
- Preview the results before opening them.

#### What We Don't Like

- Free users are limited per month.
- Results cannot be exported to a file unless you pay.
- Can't search for addresses by name.

Hunter is probably the most useful tool that you can take advantage of if you're looking for somebody's company email address.

It works by asking you to type a company domain name in the given field and then pulls up a list of all the email results it finds based on sources from around the web. Depending on the results, the tool may even suggest a pattern like *{first}@companydomain.com* if it detects any.

Once you've found an email address from the results that you want to try emailing, you can look at the icons beside the address to see Hunter's confidence score assigned to it and an option to verify. When you click to verify, you'll be told whether the address is deliverable or not.

You're allowed to perform up to 100 searches for free every month, make bulk requests for email searches as well as verification and export results to a CSV file. Premium subscriptions are available for larger monthly request limits.

Make sure to check out the [Hunter Chrome extension](#) too, which makes it possible for you to get a quick list of email addresses when you're browsing a company site. No need to open up a new tab and search Hunter.io. It even adds a Hunter button to LinkedIn user profiles to help you find their email addresses.

## **2 Use Voila Norbert to Search for Email Addresses by Name and Domain**

### **What We Like**

- Narrow results by name.
- Option to email directly.
- Can save list to a file.

### **What We Don't Like**

- Account required.
- Name and domain required.
- Limited number of searches.

[Voila](#) Norbert is another email address search tool that's both free to sign up and super easy to use.

In addition to a domain name field, you're also given the option to fill out the first and last name of the person you're trying to contact. Based on the information you provide, Norbert will start searching for related email addresses and will notify you of anything it can find.

The tool works best with company domains because there are only so many users that will have a company email address. Amazingly enough, it even works with free email providers like Gmail.

Note: Bear in mind that if you decide to search for a first and last name with a Gmail.com domain, the results that Norbert gives you may not correspond to the exact person you're trying to contact, mainly because Gmail has such a massive user base and there are bound to be multiple users who share the same names.

Like Hunter, Voila Norbert lets you search for email addresses manually or in bulk. It also has a handy Contacts tab to keep your email contacts organized and a Verification tab for verified address. You can even integrate the app with other popular business services like HubPost, Salesforce, Zapier, and others.

The major downside to this tool is that you can only make a total of 50 free requests before you'll be asked to provide payment either with a "pay as you go" plan at \$0.10 per lead or a monthly subscription for more requests.

## **3 Use Anymail Finder to Search for Email Addresses by Name and Domain**

### **What We Like**

- Can find emails in bulk.
- Easy to use.
- Results can be saved to a file.

### **What We Don't Like**

- Company-specific searches only.
- Requires both a first and last name.
- Trial version has limited features.

Anymail Finder has a few subtle differences from the above options that make it a worthwhile mention here.

You can type in any name and a domain to search for an email address right on the homepage before you sign up. The tool

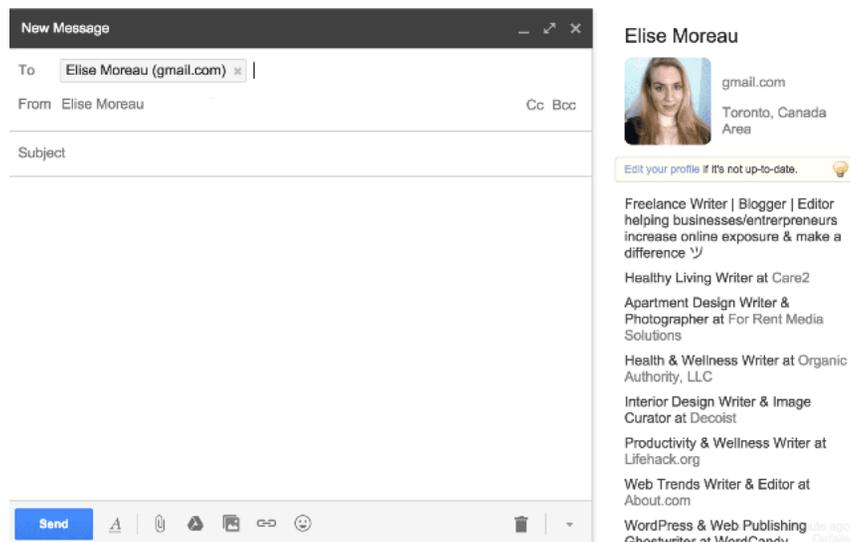
works fast and you'll get three verified email addresses beneath the search fields if it finds any.

The biggest downside to Anymail is that it's very limited in use for free users with only 20 free requests to make before you'll be asked to buy more. This tool offers users the opportunity to buy a certain number of email requests rather than operating on a monthly subscription model.

Another big downside is that Anymail Finder doesn't seem to work with free email providers such as Gmail. If you try searching for one, it will be stuck in search mode for a long time before a "We could not find this email" messages appears.

If you do decide to sign up for the free trial of 20 email requests, you'll get to search emails manually or in bulk. Anymail Finder also has a Chrome extension with some pretty good ratings.

#### 4 Use Rapportive to Find Active Email Addresses



Screenshot of Gmail.com

#### What We Like

Works seamlessly with Gmail.

Easy to install.

#### What We Don't Like

Often doesn't work or is very slow to load.

Runs in Chrome only.

Rapportive is a neat little email tool from LinkedIn that works with Gmail. It only comes in the form of a Google Chrome extension.

Once installed, you can start composing a new email message in Gmail by typing any email address into the *To* field. Active email addresses that are linked to LinkedIn profiles will display profile information on the right side.

Rapportive won't give you any suggested email addresses like any of the previous tools mentioned; that's up to you to figure out. So, you can either use one of the previously mentioned tools to come up with email addresses or you can guess them yourself by typing examples into the Gmail *To* field like *firstname@domain.com*, *firstandlastname@domain.com* or even more generic addresses like *info@domain.com* and *contact@domain.com* to see what sort of information appears in the right column.

What's great about Rapportive is that it can give you some hints about email addresses that aren't exactly connected to any social data. For example, *info@domain.com* may not be in use for a particular person's LinkedIn profile, but if you type it into the *To* field in a new Gmail message, it may display a message in the right column confirming that it's a role-based email address.

If you type in an email address that doesn't show any information in the right column, it probably isn't a valid email address.



## AI AND HUMANS

### Defense Defense

By Kathy Garges

At this time of year, the cheer “Defense Defense” can be heard rising from many American football stadiums. The same sentiment is coming from political protestors in Hong Kong, and from citizens around the globe, as they try to foil artificial intelligence surveillance by governments and police. Protestors are using AI themselves, to organize and manage protests, and sometimes to identify police they believe have violated the law.

In case you missed it, the Hong Kong protests have been going on for months. As this column is being written, China is increasing its troops there. Hong Kong is a densely-populated area that has been on a border in space and time between a politically repressive China that conducts intensive, routine surveillance of citizens, and the rest of the world (where surveillance of citizens is generally lighter or less obvious, to varying degrees). A proposed change in extradition law started the Hong Kong protests, but there is also an underlying fear that China will extend its surveillance there, ending its separate political system and remaining civil liberties.

The primary use by police of AI in the Hong Kong protests is for face recognition. Fixed surveillance cameras and police on the spot take video and then analyze it to identify protestors. It has been reported that police use violence to force protestors to open their smartphones by face identification or other biometric means (e.g., fingerprints), so they can get access to identities of other protestors and tactical information about their plans.

Protestors have developed defenses. The “button mash,” a quickly-executed macro, will convert a smartphone from biometric

login to “cop mode,” which requires entering a password. Passwords are typically harder for police to obtain. On the street, protestors wear simple surgical masks or wield umbrellas to avoid identification. Even though the AI face recognition software used in public places is far from accurate, it is a significant threat to dissidents.

Thick makeup with swoops and geometric patterns and masks are other disguise options. Polish industrial designer Ewa Nowak recently designed Incognito, a brass headpiece that outlines the hollows under the eyes, and hooks over the ears. The trouble with makeup and masks is they don’t always work to foil AI; they need to be customized to the specific machine learning face recognition software. Also, protestors who use them can be pegged for attention more easily by police at the protest scene or enroute.

Police in Hong Kong and elsewhere hide cameras in street lamps, traffic lights, and traffic cones. In Hong Kong they have been carrying cameras high on poles during clashes. Protestors are now pointing lasers at cameras, spray-painting camera lenses, and dismantling street lamps. When protestors started identifying violent police publicly (sometimes “doxxing” them by publicizing their home addresses and other private information), police stopped wearing ID badges.

Mobile phones are crucial to protestors. They often organize ad hoc, “Be Water,” protests by group chat. Smartphone data is usually encrypted (known as “going dark”), but police can get access by joining the chat. For example, Telegram, an encrypted messaging app, allows users to quickly identify family and friends who use the app by uploading phone number contact lists. There has been concern that this feature could be used by police to identify protestors, and Telegram recently announced that it will implement an option to disable this feature.

The Hong Kong protests have generated new, complex, real-time mapping systems for coordinating actions and providing information so participants can better protect themselves. Visual,

interactive maps are more effective than text in these intense situations. Hundreds of thousands of people per day may be using them in Hong Kong, including many not involved in the protests who are trying to avoid danger zones.

The mapping apps that have sprung up rely on crowdsourcing information at the scene and try to optimize speed and accuracy. Real-time data is generated by messaging, iPad, or paper and pen. The feeds are then double-checked and integrated at a control point and sent out on the internet. The maps use emoji for quick communication. A white speech bubble may represent tear gas. A dog icon can stand in for police. Since internet access can be limited in crowds, people on the edges use AirDrop software, which creates an encrypted local WiFi network, to “ripple in” the data to those inside.

Hong Kongers are not the only ones concerned about surveillance on the cyber “mean streets.” There are an estimated tens of thousands of automated license plate readers, “ALPRs,” in use in the United States alone. The government has no need to access GPS, or wait for self-driving car networks, to locate a vehicle and identify who is likely to be inside it.

At the recent DefCon in Las Vegas, Adversarial Fashion showed a line of clothing for wear by drivers and passengers that is designed to generate junk data to confuse these readers. Earlier this year, researchers at Belgian university KU Leuven demonstrated an adversarial patch that can be printed on a color printer and worn on clothing to foil a video surveillance system designed to identify whether a human is in its range, an invisibility cloak. They are working on a universal patch that will foil most surveillance systems.

Suddenly, the hottest area of AI machine learning innovation has become defending against it. The results so far show that humans are still as ingenious as our technological inventions. You might want to add some AI invisibility fashions to your personal shopping and gift lists – just in case.

### Sources and additional information:

Erin Blakemore, Taryn Salinas and Adolfo Arranz (illustrations), “The history of Hong Kong, visualized,” National Geographic, August 26, 2019, <https://on.natgeo.com/2Me2tFO>

Paul Mozur, “In Hong Kong Protests, Faces Become Weapons,” The New York Times, July 26, 2019, <https://nyti.ms/2lk9bll>.

Shibani Mahtani and Jennifer Hassan, “Hong Kong protesters are using lasers to distract and confuse,” The Washington Post, August 1, 2019, <https://wapo.st/2MeZfS1>.

Patrick Howell O’Neill, “Why smartphones’ “cop mode” might not keep cops out for much longer,” MIT Technology Review, August 6, 2019, <http://bit.ly/32XCHf9>.

Joel Schectman, “Exclusive: Messaging app Telegram moves to protect identity of Hong Kong protesters,” Reuters, August 30, 2019, <https://reut.rs/2MnPXmP>

Mary Hui, “Real-time maps warn Hong Kong protesters of water cannons and riot police,” Quartz, September 4, 2019, <http://bit.ly/2M6cCUo>.

Charlotte Jee, “A new clothing line confuses automate license plate readers,” MIT Technology Review, August 15, 2019, <http://bit.ly/331xDqe>.

Kelli Maria Karducki, “The High Fashion of Countering Facial Recognition” OneZero, September 16, 2019, <http://bit.ly/2IlyERR>.

Will Knight, “How to hide from the AI surveillance state with a color printout,” MIT Technology Review, April 23, 2019, <http://bit.ly/2ln03mx>.

Sidney Fussell, “Why Hong Kongers Are Toppling Lampposts,” The Atlantic, August 30, 2019 <http://bit.ly/2OhqiPa>.

---