# South Bay Apple MUG Macintosh

**April 2016**

A Monthly CUPFUL for South Bay Apple Mac User Group


## **Browser Fingerprinting**, by Nick Nikiforakis & Günes Acar

In July 1993, The New Yorker published a cartoon by Peter Steiner that depicted a Labrador retriever sitting on a chair in front of a computer, paw on the keyboard, as he turns to his beagle companion and says, "On the Internet, nobody knows you're a dog." Two decades later, interested parties not only know you're a dog, they also have a pretty good idea of the color of your fur, how often you visit the vet, and what your favorite doggy treat is.

How do they get all that information? In a nutshell: Online advertisers collaborate with websites to gather your browsing data, eventually building up a detailed profile of your interests and activities.

The earliest approach to online tracking made use of cookies, a feature added to the pioneering Web browser Netscape Navigator a little over a year after Steiner's cartoon hit newsstands. Other browsers eventually followed suit. Cookies are small pieces of text that websites cause the user's browser to store. They are then made available to the website during subsequent visits, allowing those sites to recognize returning customers or to keep track of the state of a given session, such as the items placed in an online shopping cart. Cookies also enable sites to remember that users are logged in, freeing them of the need to repeatedly provide their user names and passwords for each protected page they access.

So you see, cookies can be very helpful. Without them, each interaction with a website would take place in a vacuum, with no way to keep tabs on who a particular user is or what information he or she has already provided. The problem came when companies began following a trail of cookie crumbs to track users' visits to websites other than their own.

How they do that is best explained through an example. Suppose a user directs her browser to a travel website—let's call it Travel-Nice-Places.com—that displays an advertising banner at the top of the page. The source of that banner ad is probably not Travel-Nice-Places.com itself. It's more likely located on the Web servers of a different company, which we'll call AdMiddleman.com. As part of the process of rendering the page at Travel-Nice-Places.com, the user's browser will fetch the banner ad from AdMiddleman.com.

continued on page 4

## March 30 Meeting
## El Capitan

Jim Pernal will discuss the latest Mac Operating System El Capitan (10.11) The presentation will include the requirements for using this system, how to upgrade, why you should upgrade, and finally a few of the new features in the system with some demos. Also, Tom Thorpe will continue his series on Internet Basics with a short presentation titled *IP Addresses*.

Don't miss the meeting! See page 2 for details.

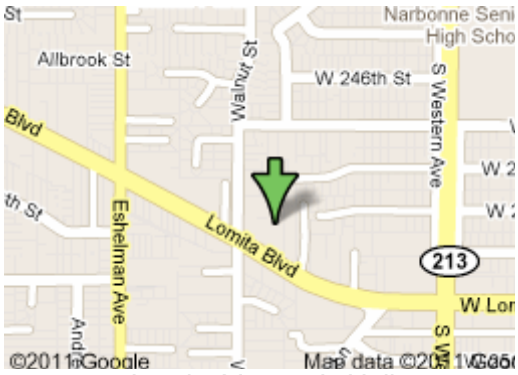
## Donations

Thanks to Gundula Schneider for her donation of an HP printer to the Girls and Boys Club of LA Harbor. If you have computer equipment to donate (used but functional), contact Pete Myers: pjmyerz@gmail.com.

IN THIS ISSUE

# Welcome to the SBAMUG
# South Bay Apple Mac User Group

Members,friends and colleagues are invited to attend our monthly meetings (usually the last Wed of the month). The $35 annual membership dues entitle you to receive this monthly newsletter by mail or online, plus many more benefits (page 8). To become a member or get more info please check our websiite.



Lomita Veteran's Hall,
1865 Lomita Blvd, Lomita

Meetings: Lomita Veteran's Hall,
1865 Lomita Blvd, Lomita
Mail: PO Box 432, Redondo Beach, CA
90277-0432
Phone: (310) 644-3315
Email: info@sbamug.com
Website: http://www.sbamug.com/wp

## SBAMUG Meeting Format:

**6:30—7:30 p.m.** Questions & Answers and Sharing: *Everyone* is welcome, beginners encouraged
**7:30—7:50 p.m.** 'iSocial' – shoot the Mac breeze with others over a cookie*
**7:50—8:00 p.m.** Announcements
**7:50—9:00 p.m** Program
**Refreshments provided; donations appreciated!*
Submit suggestions for topics or speakers, or articles, ideas & original artwork for this newsletter to pjmyerz@gmail.com by the last Wednesday of each month. Articles may be edited to fit space.

## Officers & Volunteers:

President: Kent McDonald VP: open
Secretary: Wayne Inman Treasurer: CW Mitchell
Directors at Large: Dave Nathanson, Margaret Wehbi, Arnold Silver, George Wilde, Joan King, Clarence Baisdon, Pete Myers
PD Disk Editor: Jim Pernal
Membership: CW Mitchell
Member Development: Pete Myers
Programming: Kent McDonald
Greeter: open
Server Director: Dave Nathanson
Newsletter: Pete Myers, Bill Berks
USPS Liaison: CW Mitchell
Refreshments: Arnold Silver/member contributions

## SBAMUG Monthly Calendar

Mar 30: El Capitan
April 27: iOS 9 Basics

### Other Meetings:

- 1st Wed each month – SBAMUG Core Group, 7:30 pm. Join Google+ SBAMUG community, or email: info@sbamug.com.
- Special interest groups (SIGs): Feb 16 on iPhone; contact Glen Terry: gterry@me.com
- Last Sat. each month - Northrop Grumman-Ham Radio & Computer Swap Meet, 7--11:30 a.m. Meet at SE corner of Marine/Aviation Blvd, Redondo Beach
- Los Angeles Portable Users Group: Mac OS X, iPhone, iPod, MacBook, etc., http://www.lapug.org/
- Find more: http://www.apple.com/usergroups/

### Membership Report – 98 members!

*Please wear membership card as your name tag*
**Welcome New Members:** Carlos Marques, Sharon Ratterre.
**Thank You Member Renewals:** Dave Moorhead, Philip Gruskin, John Kells, Bob Lay, Erik Nilsson, Allan Boodnick, Paul Curry, Robert Goodman,Victor Kosuda, Margaret Wehbi.
If your name is not spelled right or your expiration date is wrong, contact cwmitchell@sbamug.com for correction. Or contact CW for everything membership, dues and benefits.
Please watch for your renewal letter, then sign and date it and return it with $35 check (in enclosed self-addressed envelope) or bring letter with payment to meeting.

THE SOUTH BAY MUG (ISSN 1058-7810) is published monthly for $35 per year by South Bay Apple Mac User Group, 2550 Via Tejon, Suite 3J, Palos Verdes Estates, CA 90274. Periodicals postage paid at Palos Verdes Peninsula, CA and at additional mailing offices. POSTMASTER: Send address changes to THE SOUTH BAY MUG, P.O. Box 432, Redondo Beach, CA 90277-0432.

## SBAMUG March 2016 PD CD

This is the March CD article. Seven items this month. Okay, some hope for those still back on OS X 10.7 since several of these programs will work on that system.

**Cyberduck-4.8.1.19040.zip** For those who need to move items to and from websites. FTP and SFTP. Free. OSX 10.7.3+ Intel

**ccc-4.1.7.4285.zip** Carbon copy cloner. Backup your hard drive and also make bootable clones of your drive so that you can immediately reboot to the cloned drive and continue. $39.95. OSX 10.8 +

**Mactracker_7.5.4.zip** A free database on all the Macs Apple has made. Plus has mice, keyboards, displays, printers, etc. Intel 10.7+

**Opera_NI_stable.zip** Alternative web browser. Has extensions and speed dial. Intel 64 bit 10.7+ Free.

**PDFExpert.dmg** Read, annotate, fill, and sign PDF documents. Type for a handwritten like signature, or this can record your actual signature on a trackpad. OSX 10.10+ Shareware, $19.99

**TextExpander.zip** One of Allison Sheridan's favorite programs. Expand keyboard shortcuts into longer text snippets, or a picture. Saves typing. OSX 10.10+ Shareware, $44.95.

**TGPro_2_9_7.zip** Final item this month is a utility to control fan speeds, monitor temperatures, and even find faulty temperature sensors in your mac. Intel 64 bit 10.7+ Shareware, $16.00.

See you at the March meeting. The PD CD will be the combined March-April one, available at the April meeting.

## Chat Room

At the February meeting, by a show of hands, many indicated that they were not members of the SBAMUG email group. This was surprising because of the numerous advantages of joining the group:

- Get MUG meeting and SIG announcements
- Learn about MUG website posts
- Request technical help
- Participate in discussions and respond to technical help requests

The volume of mail is not excessive and you will not get a bunch of junk mail. To join, go to http://www.sbamug.com/wp/our-sbamug-email-group/ and follow the directions under the heading **How Do I Join/Subscribe to the group?**

The tech press is almost 100% behind Apple in its dispute with the FBI. Here's a contrary opinion from Mike Isaac of the NY Times: "A year or so ago, Apple took the deliberate step of making it so it could not gain access its own phones at the behest of the government, and it is only accelerating that effort. And I've already reported they're going to take similar steps with iCloud and generally embrace this approach overall. That's drastically different than Apple's history of complying with government requests for data when it is legally required to do so."
"So when the company bound its own hands, I have to ask: What did it expect the government to do, just sit back and say, "Oh, well, I guess we won't request any more data." Of course not. This is an escalation in a continuing war for reach into consumer data, and now it's going to court."
"I think, in general, people don't want the government snooping on their data. However, I think this is perhaps the absolute worst case Apple and others chose to push back on, considering that it includes questions of terrorism and the mass slaughter of innocents. Tracking down terrorist ties to murderers is far easier for normal, non-techie people to comprehend than the intricacies of software and data extraction."

Independent software developer, Reggie Ashworth has announced the release of AppDelete 4.2.4, an update to his very popular application deletion utility for Mac OS X. With a simple Drag & Drop, AppDelete will uninstall anything along with all of the associated items. Mac users will no longer have to hunt through their system to find and delete these items manually. AppDelete 4.2.4 is only $7.99 (USD) for a single user license. Upgrades from Version 2/AppDelete Lite are only $3.99 (USD). A full-featured demo is available.
http://prmac.com/release-id-78682.htm

Browser Fingerprinting, from page 1

Here's where things get sneaky. The Web server of AdMiddleman.com sends the requested banner ad, but it also uses this opportunity to quietly set a third-party cookie on the user's browser. Later, when that same user visits an entirely different website showing another ad from AdMiddleman.com, this ad supplier examines its previously set cookie, recognizes the user, and over time is able to build a profile of that user's browsing habits.

You might ask: If this brings me more relevant online advertisements, what's the harm? True, online tracking could, in principle, help deliver ads you might actually appreciate. But more often than not, the advertisers' algorithms aren't smart enough to do that. Worse, information about your Web browsing habits can be used in troubling ways. A car dealer you approach online and then visit in the flesh, for example, could end up knowing all about your investigations, not only of its inventory but of all the other car-related websites you've been checking out. No wonder such tracking has garnered a reputation for being creepy.

Not long after the use of third-party tracking cookies became common, various media outlets and privacy organizations began questioning the practice. And over the years, people have increasingly come to appreciate that the set of websites they visit reveals an enormous amount about themselves: their gender and age, their political leanings, their medical conditions, and more. The possession of such knowledge by online advertising networks, or indeed by any company or government agency that purchases it from those networks, comes with potentially dire consequences for personal privacy—especially given that users have no control of this very opaque process of data collection.

It should come as no surprise that some of the early news articles about advertisers' use of cookies had headlines announcing "the death of privacy" and made allusions to George Orwell's all-seeing Big Brother. Even the programmers and engineers involved in the development of technical standards got an earful.

In particular, in 1997 a coalition of privacy organizations wrote an open memo to the Internet Engineering Task Force (sending copies to the leading browser developers) that expressed their support for the first cookie standard, RFC 2109, which stated that third-party cookies should be blocked to "prevent possible security or privacy violations." But advertising companies pushed back harder. And in the end, neither of the two mainstream browsers of that era, Netscape Navigator and Internet Explorer, followed the specification, both allowing third-party cookies.

The winds began to shift in 2005, though, when browser developers started adding a "private browsing" mode to their products. These give users the option of visiting websites without letting those sites leave long-term cookies. Independent developers, too, started producing privacy-preserving extensions that users could add to their browsers.

But when people started deleting their cookies, the companies involved in tracking didn't just roll over. They responded by developing new ways of sniffing out users' identities. Most had one thing in common: They tried to bury the same tracking information found in cookies in some other corner of the user's browser.

As you might expect of this long-standing cat-and-mouse game, the advertising networks have not sat idle. In recent years, they have shifted to a form of tracking that doesn't require Web servers to leave any kind of metaphorical bread crumb on the user's machine. Instead, these ad networks rely on a process known more generally as device fingerprinting: collecting identifying information about unique characteristics of the individual computers people use. Under the assumption that each user operates his or her own hardware, identifying a device is tantamount to identifying the person behind it.

While this all sounds very sinister, it's important to realize that such fingerprinting has some very benign, indeed laudable, applications. It can be used, for example, to verify that someone logging into a Web-based service is not an attacker using stolen log-in credentials. Fingerprinting is also helpful for combating click fraud: Someone displays an advertisement on his website in return for payment each time that ad is clicked on—and then tries to run up the bill by having an identity-feigning computer click many times on the ad. The problem is that fingerprinting has become so precise that it makes a sham of browsers' privacy-protection measures.

We have examined not just what kinds of fingerprinting are theoretically possible but, more to the point, what is actually going on in the wilds of the Internet's tracking ecosystem. We started our analysis at the University of Leuven, in Belgium, by first identifying and studying the code of three large fingerprinting providers: BlueCava, Iovation, and ThreatMetrix.

The results were rather chilling. For instance, we found that one company uses a clever, indirect method of identifying the installed fonts on a user machine, without relying on the machine to volunteer this information. We also discovered fingerprinting code that exploits Adobe Flash as a way of telling whether people are trying to conceal their IP addresses by communicating via intermediary computers known as proxies. In addition, we exposed Trojan horse–like fingerprinting plug-ins, which run surreptitiously after a user downloads and installs software unrelated to fingerprinting, such as an online gambling application.

With the information we gathered about these three companies, we created and ran a program that autonomously browses the Web and detects when a website is trying to fingerprint it. The purpose of this experiment was to find more players in the fingerprinting game, ones less well known than the three we studied initially.

We quickly uncovered 16 additional fingerprinters. Some were in-house trackers, used by individual companies to monitor their users without sharing the information more widely. The rest were offered as products by such companies as Coinbase, MaxMind, and Perferencement.

continued on page 5

Browser Fingerprinting, from page 4
And it seems the companies selling this software are finding buyers. Our results showed that 159 of Alexa's 10,000 most-visited websites track their users with such fingerprinting software. We also found that more than 400 of the million most popular websites on the Internet have been using JavaScript-only fingerprinting, which works on Flash-less devices such as the iPhone or iPad. Worse, our experiment revealed that users continue to be fingerprinted even if they have checked "Do Not Track" in their browser's preferences.

Browser fingerprinting is becoming common, and yet people are mostly in the dark about it. Even when they're made aware that they're being tracked, say, as a fraud-protection measure, they are, in essence, asked to simply trust that the information collected won't be used for other purposes. One of those is targeted advertising, which works even when users switch into their browsers' private mode or delete their cookies. What are those unwilling to go along with this new form of tracking doing about it?

As part of our research on browser fingerprinting, we examined various tools that people are using to combat it. One popular approach is installing browser extensions that let you change the values that identify your browser to the server. Such modifications allow users to occasionally trick servers into dishing out pages customized for different browsers or devices. Using these extensions, Firefox devotees on computers running Linux, for example, can pretend to be Internet Explorer fans running Microsoft Windows. Other extensions go further, reporting false dimensions for the screen size and limiting the probing of fonts.

Our analysis showed that a mildly accomplished fingerprinter could easily overcome any of these supposedly privacy-enhancing browser extensions. That's because modern browsers are huge pieces of software, each with its own quirks. And these idiosyncrasies give away the true nature of the browser, regardless of what it claims to be.

This makes those privacy-protecting extensions useless. In fact, they are worse than useless. Installing such a fingerprint-preventing browser extension only makes you stand out more.

Given that advertising is the Web's No. 1 industry and that tracking is a crucial component of it, we believe that user profiling in general and fingerprinting in particular are here to stay. But more stringent regulations and more effective technical countermeasures might one day curb the worst abuses.

We and other researchers are indeed trying to come up with better software to thwart fingerprinting. A straightforward solution might be to stop the fingerprinting scripts from ever loading in browsers, similar to the way ad blockers work. By maintaining a blacklist of problematic scripts, an anti-fingerprinting extension could detect their loading and prohibit their execution.

One challenge is that the blacklist would have to be revised constantly to keep up with the changes that trackers would surely make in response. Another issue is that we don't know whether the loading of fingerprinting scripts is necessary for the functionality of certain websites. Even if it's not required now, websites could be changed to refuse loading of their pages unless the fingerprinting scripts are present and operational, which would discourage people from trying to interfere with them.

A more effective way of approaching the problem would be for many people to share the same fingerprint. To some extent that is happening now with smartphones, which can't be customized to the degree that desktop or laptop computers can. So phones currently present fewer opportunities for fingerprinters. It might be possible to make other kinds of computers all look alike if Web browsing were done through a cloud service, one that treats the browser running on the user's PC simply as a terminal. Trackers would then be able to detect only the cloud browser's fingerprint.

Companies offering cloud-based browsing already exist, but it's not clear to us whether the browsers that are exposed to potential fingerprinters actually operate in the cloud. Still, there's no reason to think that a system for preventing fingerprinting with a cloud browser couldn't be engineered. For some of us, anyway, it could be worth adopting, even if it involved monthly charges. After all, doing nothing has a price, too—perhaps one as steep as forfeiting online privacy for good.

## ***Tips and Myths About Extending Smartphone Battery Life,*** *by Brian X Chen*

Ashlei Temeña's family trip to Disneyland last Thanksgiving break turned into a nightmare when her smartphone battery hit empty. Ms. Temeña, a San Francisco support technician, had gotten separated from her family and realized she had no way to find anyone. Instead of riding roller coasters, she wandered around searching for the group — eventually locating them four hours later watching fireworks. "I wanted to throw my phone on the ground by the end of the day," Ms. Temeña said. Many consumers can relate. Despite the leaps forward in mobile phone technology with crisp, clear screens and faster chips, batteries have made only sluggish progress. That has propelled a desire for longer battery life to the top of the list of factors considered by consumers when they purchase smartphones, according to a 2014 survey by the research firm IDC.

So why is battery technology still underwhelming? Plenty of companies have been developing smarter battery technology for years, including methods to increase battery capacity tenfold or charge devices by pulling energy from the air. But lithium ion, the technology that most mainstream batteries are based on, is low cost and easily

continued on page 6

Battery Life, from page 5

reproducible while being safe — so we'll be stuck with it for the foreseeable future. In general, lithium ion improves about 10 percent a year in terms of the amount of energy that can be stored in a given space, which is partly why consumers perceive batteries as being far behind other technologies. With that backdrop in mind, we ran an array of tests to determine best and worst practices for preserving battery life on smartphones. Here are eight tips and seven myths busted by our findings:

1. Use auto-brightness for the screen.

A smartphone's screen consumes more energy than any other component, so the easiest way to cut down battery drain is to reduce your screen brightness. In an hourlong test, an iPhone 6s used 54 percent less battery power with the screen brightness at minimum as compared with maximum brightness. But it's tough to use a dim screen in bright environments, so most phones offer an auto-brightness mode that automatically adjusts the screen's brightness based on ambient light. We found that enabling auto-brightness saved a good amount of battery life.

2. Block power-sucking ads.

When browsing the web, your smartphone also burns through power when it downloads mobile ads on websites. Installing an ad blocker will greatly extend battery life. We ran a test that cycled through a list of websites for two hours over a Wi-Fi connection. Safari on an iPhone 6s used 18 percent of a full battery. Installing the 1Blocker ad blocker reduced battery usage for the same test to only 9 percent of a full battery.

3. Tweak your email settings.

Email can have a major impact on battery life if you have multiple email accounts and receive lots of email. Your smartphone can update your email automatically using a technology called push, which brings new messages to your phone the instant they are transmitted. Push can be a power hog because it requires your phone to constantly listen for new messages, so if you get a lot of email, there's a good chance your phone is using lots of energy.

4. Play downloaded music instead of streaming.

The next tip may come as unwelcome news. Nowadays, online streaming is the most popular way to listen to music, with services like Spotify, Pandora and Apple Music — but this method guzzles lots of battery power. In the Wirecutter's tests, streaming music over a Wi-Fi connection for two hours used 10 percent of an iPhone's battery reserves; streaming the same music stored directly on a device over two hours consumed only 5 percent. Fortunately, streaming services like Spotify and Apple Music still let you listen to songs the old-school way: by storing the music right on your device.

5. Turn off wireless when reception is poor.

You may have noticed that when you're in a place without good Wi-Fi or cellular coverage, your phone's battery seems to drain much more quickly. That's because the phone uses energy searching for a good signal and, if the signal is very weak, trying to get a better connection.

To conserve battery life, disable the phone's wireless circuitry. Airplane Mode, an option that will turn off all wireless features, is a quick and easy solution in areas with poor reception.

6. Check the battery usage lists.

Consumers can get even better results with a bit of sleuthing. There is a simple way to see which apps are using a lot of battery power: open the Settings app and in the Battery menu, there are sorted lists of apps that are using the most energy. On the battery usage screen, tap the clock button to reveal information about how much of your battery life each app is consuming when you're actively using the app ("screen") compared with when you're not ("backgd").Be on the lookout for apps that are active for extended periods in the background and are using a lot of battery power. If you find apps using up lots of energy in the background, disable their background activities. Go to the Settings app, tap General and then Background App Refresh and disable the background activities for any apps.

7. Disable unnecessary location tracking.

Watch out for apps that track your location. Your phone's GPS circuitry, which determines your geographic location for mapping and fitness features, consumes a lot of battery power. A run-tracking program that monitors your precise location for the duration of an hourlong run will lower your battery level. If a location-based app is using a lot of power, especially in the background, there's a good chance the app is using GPS, Wi-Fi and the phone's sensors frequently. You can decide whether to disable location features for it (either via your phone's Location Services settings, or by changing settings in the app itself). You can disable the app's ability to track your location by going to Privacy menu and Location Services.

8. Shut off unnecessary push notifications.

Both Apple and Google recommend disabling push notifications, which are essentially app alerts, to conserve battery life. Notifications require regular communication with notification servers, and each notification causes your phone to wake up for a few seconds, including turning on the screen, to show you a message and give you a chance to act on it.

**Beware battery-saving myths.**

1. Closing unused apps.

continued on page 7

Battery Life, from page 6

There is plenty of inaccurate conventional wisdom about methods to prolong battery life. Let's start with one of the worst "tips": Closing (or force-quitting, as it's commonly called) apps you are not currently using. The theory is that apps running in the background are using your phone's components, so quitting them will save energy. While that may be true on a computer, smartphones are designed differently: Once an app is no longer in the foreground — meaning you are not actively using it — most or all of its processes are frozen. In other words, while an app may still be loaded in a phone's memory, it probably is not doing much in the background to drain your battery.

.2. Don't assume turning off Wi-Fi will always help.

A common suggestion for extending battery life is to disable Wi-Fi. However, if you're in range of a strong Wi-Fi signal, your phone uses less energy to connect to the Internet with a Wi-Fi connection than a cellular one. If you regularly use apps that rely on your location, having Wi-Fi enabled helps your phone determine its location without having to rely solely on power-hungry GPS features, so it actually helps a battery last longer. An exception is when you're at the edges of a Wi-Fi network, where your phone is struggling to get a good connection, *and* you have a good cellular data connection. But in most cases, you're usually better off keeping Wi-Fi enabled.

3. Avoid disabling all location services.

Many apps that use your location do so only intermittently. Even using the Maps app for short navigation sessions doesn't use more than a few percent of your battery's capacity — and having the phone's screen continually on is a big part of why navigation uses a lot of power. In other words, don't disable all of your phone's location-based features just to extend your battery life.

4. Don't always choose Wi-Fi over cellular.

Many people, and even smartphone vendors such as Apple, claim that using Wi-Fi for wireless data consumes less power than using a cellular signal, so you should use Wi-Fi whenever you can. However, the Wirecutter's testing found this isn't always the case. In testing in a location where both Wi-Fi and cellular LTE signals were strong, an hour of browsing over Wi-Fi used roughly the same amount of battery power as an hour using LTE on an iPhone.

5. Let Siri and Google listen for your commands.

Both iPhones and Android phones include a hands-free feature for summoning their virtual assistants by speaking voice commands. You can just say "Hey Siri" to the iPhone or "O.K. Google" and then speak your request or command. While convenient, this feature requires your phone to constantly listen for that special phrase, which uses some power.

Yet if you have one of the phones that supports this feature, disabling it won't conserve much battery life. In the Wirecutter's testing with an iPhone 6s Plus and a Nexus 6P, there was a negligible difference in battery usage between having the always-on virtual assistant enabled or disabled over a two-hour period.

6. Don't forgo third-party chargers made by reputable vendors.

A common warning around the Internet is that you should use only the charger that came with your phone, otherwise you could damage your phone's battery. In reality, the phone itself contains all the circuitry responsible for charging its battery. The AC adapter (as it's more accurately known) simply converts the AC current from a wall outlet into low-voltage, low-amperage DC current that it provides via a USB port. This is why you can also charge your phone using the USB port on a computer, a USB battery pack or a charger in your car — the phone is designed to allow it to charge from a variety of power sources that can produce a wide range of current.

7. Calibrate only occasionally.

For many years, devices that used rechargeable batteries required "conditioning" or "calibrating," a procedure that prevented the battery from forgetting how much capacity it actually had. Today's smartphone batteries no longer suffer from this issue.

What can happen, however, is that the phone itself loses track of how much capacity its battery has: Every battery gradually loses capacity over time as you use and recharge it, and the phone's software isn't always good at accounting for this capacity change. By periodically (once every couple of months) fully charging the phone and then using it until it dies, your phone's software will determine the battery's current capacity and thus let the phone better estimate how long it will last on a charge. In other words, the battery won't last any longer, but the phone's battery meter will be more accurate. If you find that your phone claims you have 80 percent of a charge left, but it dies a few hours later, you should try this procedure.

If all else fails ...consider buying an external battery. These accessories — which can take the form of a bulky case with a built-in battery that you wear on the phone, or a separate battery pack that connects to your phone with a cable — can provide power to last an additional few hours at the end of the day, or even to fully charge your phone's battery.

http://www.nytimes.com/2016/02/25/technology/personaltech/tips-and-myths-about-extending-smartphone-battery-life.html

**PERIODICALS**

**SOUTH BAY APPLE MAC USER GROUP**
**P.O. BOX 432**
**REDONDO BEACH**
**CA 90277-0432**

***Join, Renew or Give a Gift of a SBAMUG Membership!***

**For only $35/year you get:**

- Monthly meeting program
- E-mail group help
- Monthly newsletter (We publish 11 issues per year!)
- Use our Wiki
- Free web space & e-mail on our server
- Build your own website
- Create your own blog
- Special merchant discounts
- $$$
- Occasional swaps, free software, raffles

http://www.sbamug.com/join.html
Or, contact Membership Chair
CW Mitchell at
cwmitchell@sbamug.com

**SBAMUG Membership Application**

South Bay Apple Macintosh User Group provides you with a local source of shared knowledge & experience through monthly meetings, trainings & monthly newsletter.

**Individual & family membership: $35/year payable to SBAMUG**
**☐ New Member ☐ Member Renewal**

Name:_____

Address:_____

City:_____ State:_____
Zip:_____

Phone: (_____)_____

Email
Address:_____

Special
interest:_____

Devices you use most:_____

How did you hear about
SBAMUG:_____

Comments:_____

_____

Signature:_____

Date: _____

***Bring your Application and Fee to our General Meeting at Lomita Veteran's Hall, 1865 Lomita Blvd., Lomita.***
***Or Mail to: SBAMUG, PO Box 432, Redondo Beach, CA 90277-0432***