July 2024
Vol. XLIII, No 7

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral July 16th Meeting

Please see your membership email for the links to this month's Zoom meeting or email us at KeystoneMacCentral@mac.com.

During our program this month we plan to discuss

- ❖ Organizing your computer
- ❖ Recap June's WWW

We have virtual meetings via Zoom on the third Tuesday of each month.

Emails will be sent out prior to each meeting. Follow the directions/invitation each month on our email — that is, just click on the link to join our meeting.

Contents

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. **The *Keystone MacCentral printout*** is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2024, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

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

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

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

by Glenn Fleishman

Find Hidden Cameras While Traveling

Earlier this year, Airbnb announced a policy change that bans cameras inside properties listed by their hosts. If you haven't used Airbnb or read the fine print on its policies, you might have thought, "What the blank! Airbnb hosts could snoop on their guests?!"

Sort of. Airbnb's previous policy allowed indoor cameras only in a rental's public spaces (such as a living room or front hallway) and only when disclosed. In 2018, the company went a step further by requiring hosts to detail camera locations and where they were pointed, and by making guests acknowledge that they had seen the information by confirming via a popup dialog when booking. Apparently, that wasn't enough: as of 1 May 2024, Airbnb joined competitor VRBO in a total ban on indoor cameras.

What prompted this ban? Airbnb didn't say, and no reporting on the policy revision suggested a specific reason. The company's statement says: "The update to this policy simplifies our approach and makes clear that security cameras are not allowed inside listings, regardless of their location, purpose or prior disclosure."

Reading between the lines, I expect Airbnb may be reacting in part to the widespread availability and easy deployment of tiny, nearly invisible cameras hidden in ordinary objects you'd expect to find in a home or rental. Such objects include smoke detectors, USB power adapters, AC outlets, clock radios, tissue-box holders, appliances, and all manner of other things. As you can see by those links, they're readily available from major online retailers.

From a host's standpoint, I understand the temptation to want a hidden camera for peace of mind about the misuse of a rental. Short-term renters may bring in more people than allowed by the agreement, stage parties, or trash the place. Yet the expectation of privacy and legal protections should be paramount, and hosts should understand that. Disclosed cameras are still allowed outside, so a host could have cameras capturing entry points if they were really concerned. Indoor decibel meters that don't record conversations are also allowed in shared spaces if disclosed.

Hidden cameras are installed in lots of non-rental scenarios, of course. Though it's impossible to know for sure, the majority—maybe the vast majority—are likely deployed to watch household employees or contractors, like nannies or tradespeople. But some significant subset is for prurient and exploitative purposes. The very ugliness of the subterfuge of the disguises used for routine devices found in bedrooms and bathrooms makes that clear. It's always wrong and often criminal. Sometimes such hidden cameras are used in unexpectedly terrible ways.

By having a total ban on indoor cameras, Airbnb makes it easier for savvy travelers to examine their surroundings and report a host (and get a refund, with hotel nights picked up by Airbnb) for violations. Airbnb policy has always said, "Intentionally concealed recording devices (such as hidden security cameras) are never permitted," but with cameras allowed in some spaces and not others, there could have been gray areas.

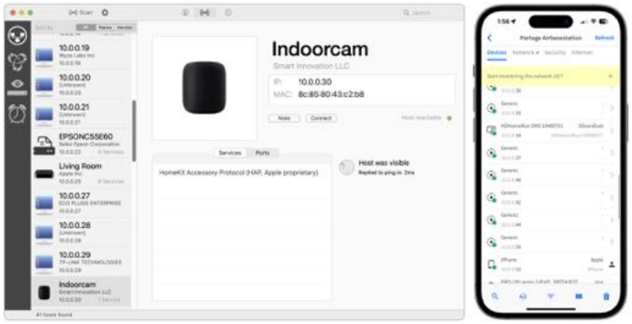
Even if you never use Airbnb, VRBO, or similar non-hospitality industry rooms, be aware that hidden cameras have also been found in hotel rooms, cruise ships, public facilities, and elsewhere. Without encouraging paranoia, it's worth being aware of the potential for privacy invasions. A particularly egregious case last year involved a flight attendant allegedly taping a poorly hidden iPhone to a toilet seat; most hidden cameras are far better obscured.

You aren't helpless in the face (or lens) of technology. If you want to check for hidden cameras, try these techniques:

- Examine anything with a reflective glass or plastic cover or with holes, such as the front screen of an alarm clock or a smoke detector. Can you spot a camera lens? Point a phone flashlight to see if it reveals a telltale reflection.

- Make the room dark by turning off all the lights. Some cameras produce visible lights.
- With the lights off, open the Camera app on your iPhone and scan the room through the viewfinder to see if you can spot an infrared or “night-vision” LED, a common attribute of spycams to improve low-light recording. To test if your iPhone’s front- or rear-facing cameras can detect infrared light in a dim room, point an infrared TV or stereo remote at the iPhone while pressing buttons.

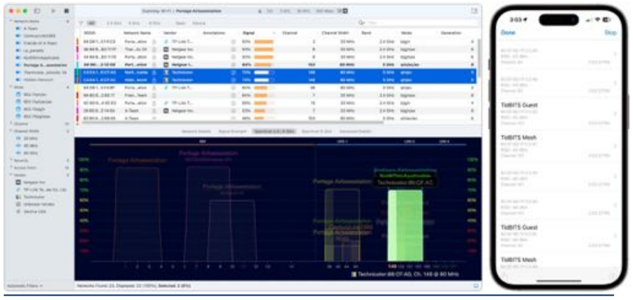
- While connected to a rental or hotel Wi-Fi network, use a passive network scanner to look for cameras. This technique is far from guaranteed, but it may reveal networked cameras. I have three cameras on my home network (one outside and two inside pointing out), and the $29.99 [iNet Network Scanner]() for macOS identifies two of them using its database of devices. The $9.99 version of [iNet Network Scanner]() for iOS produced slightly different results. Many people recommend [Fing](), a multi-platform scanner with an iOS version. When I tried Fing’s free tier, it didn’t provide sufficient identifying details about my cameras.



IP: 10.0.0.30
MAC: 8c:85:80:43:c2:b8

HomeKit Accessory Protocol (HAP, Apple proprietary)

- iNet Network Scanner showing cameras (left), Fing not identifying them (right)
- Some security experts think if you’ve gone as far as the previous step, you should also scan for additional telltale Wi-Fi networks that spycams might be connected to. There’s evidence that poorly designed camera hardware may continuously broadcast a revealing Wi-Fi network name that should be present only during setup—those network names may be a jumble of hexadecimal but can also be as obvious as starting with “IPCam.” To find such networks, use a Wi-Fi scanning app that displays signal strength: a strong signal emanating from an otherwise innocuous object could indicate a hidden camera. On a Mac, turn to the $19.95 [WiFi Explorer]() (which has a 3-day free trial and is also available in [Setapp]()) for a thorough snapshot. In iOS, Apple prevents third-party apps from revealing diagnostic Wi-Fi network information, but its outdated AirPort Utility app has a scanning mode that still works in iOS 17. [Download AirPort Utility]() and turn on Settings > AirPort Utility > Wi-Fi Scanner. Then, in AirPort Utility, tap Wi-Fi Scan in the upper-right corner and tap Scan. A lower RRSI number indicates a stronger network signal—that is, -39 dBm is stronger than -56 dBm (closer to 0).



- WiFi Explorer (left) and AirPort Utility (right) can both sort by signal strength and reveal Wi-Fi networks that don't broadcast a network name.
- If you have a personal or professional need for more thorough checking—you're being stalked, are a political protester, or are famous—you can purchase specialty devices that range from [$21](#) to [$500](#) that can help pinpoint wireless transmissions, as all these hidden cameras send data wirelessly.

The scourge isn't hidden cameras. It's human beings. While Airbnb's move won't prevent people from doing creepy things, it draws a line in the sand for acceptable behavior and clarifies that cameras may only be used outside.

Don't take this article as encouraging paranoia—it's unlikely that any given rented room or house would contain prurient hidden cameras. But if you have reason to be concerned or want extra peace of mind, you now have a handful of ways to identify such devices.

By Adam Engst

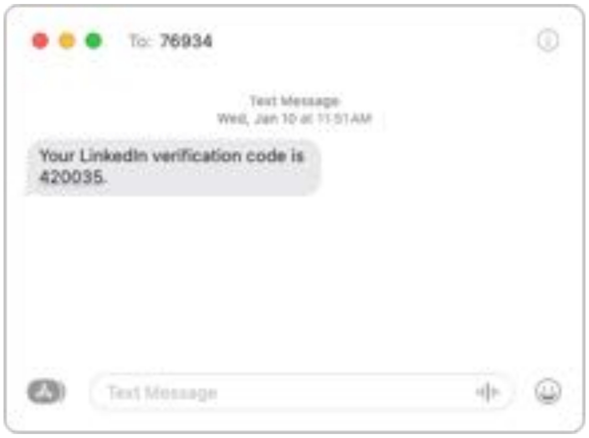
Reacting to Unsolicited Two-Factor Authentication Codes

I have long encouraged the use of two-factor authentication (2FA) or two-step verification (2SV) with online accounts whenever possible (for more about the difference, see "[Two-Factor Authentication, Two-Step Verification, and 1Password](#)," 10 July 2023). Either one is a huge security win because, after entering your password, you must enter an authentication code to complete the login.

I standardized as many of my authentication tokens in 1Password as possible because it enters them automatically for me (see "[LastPass Publishes More Details about Its Data Breaches](#)," 3 March 2023), but many online services continue to rely on SMS text messages due to their ease of use, even though authentication apps are more secure than SMS. Don't let a site's reliance on SMS dissuade you from turning on two-factor authentication—2FA via SMS is still far more secure than not using 2FA.

The most common problem with SMS is an attack called [SIM swapping](#). An attacker poses as the victim and convinces the carrier to port a phone number to a new device, effectively taking over the victim's communications. It requires knowing the victim's username and phone number, as well as additional identifying information like the last four digits of a Social Security Number. Unfortunately, information like that regularly shows up in corporate data breaches, such as the recent [Ticketmaster breach of personal data and financial details from 560 million users](#).

More commonly, you may receive an SMS text message containing a 2FA code you didn't request. This one caused me a brief moment of concern earlier this year, and a friend asked me about one they received more recently.


To: 76934

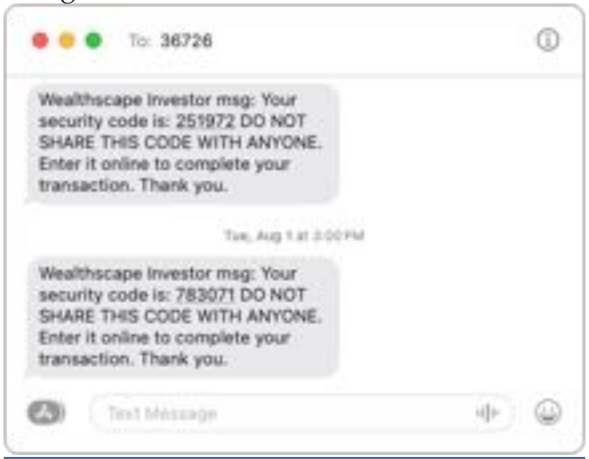
Text Message
Wed, Jan 10 at 11:51 AM

Your LinkedIn verification code is 420035.

What should you do if you get an unsolicited 2FA code? In order:

1. Don't panic. Receiving the code indicates that someone is trying to access your account and has your password, but the additional authentication step has prevented your account from being compromised.

2. Never share an authentication code with anyone! A hacker may try to access your account, be blocked by two-factor authentication, and then email, text, or even call you with a trumped-up request for the code. Since authentication codes have a short lifespan, any such contact will typically happen right away. Many companies include advice against sharing along with their codes.


To: 36726

Wealthscape Investor msg: Your security code is: 251972 DO NOT SHARE THIS CODE WITH ANYONE. Enter it online to complete your transaction. Thank you.

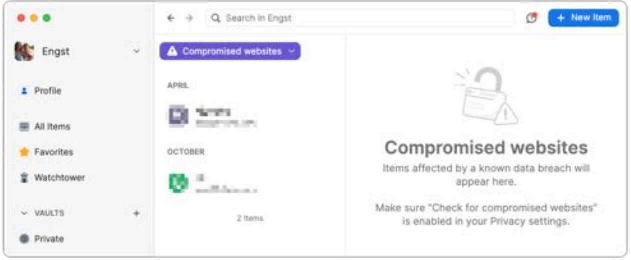
Tue, Aug 1 at 3:00 PM

Wealthscape Investor msg: Your security code is: 783071 DO NOT SHARE THIS CODE WITH ANYONE. Enter it online to complete your transaction. Thank you.

3. Change your password without clicking a link in the message. Navigate manually to the account's website, sign in, and change your password. Make sure the new password is strong, unique, and stored in your password manager. If the account in question relied on an old password that you also used for other accounts, which was common practice long ago, change the passwords on those accounts as well.

What does it mean if you receive an unsolicited 2FA code via SMS? Here are the main possibilities:

- Stolen credentials: The most common and worst-case scenario is that your email address and password were stolen, likely in a data breach, and the attacker is testing to see if they can get in. The Have I Been Pwned site is worth checking to see how many breaches you've been caught up in, but features like 1Password's Watchtower are more helpful for identifying particular sites whose passwords should be changed. Other password managers have similar features. Always change passwords on breached sites.



APRIL

[redacted]

OCTOBER

[redacted]

2 Items

Compromised websites

Items affected by a known data breach will appear here.

Make sure "Check for compromised websites" is enabled in your Privacy settings.

- Identity theft: I'm having trouble working out all the steps here—I'm not a cybercriminal!—but it feels like there's an identity theft attack vector that could result in you receiving unsolicited 2FA codes. I can imagine circumstances where an attacker had compromised your email and wanted to set up a new account impersonating you, but couldn't finish the process without entering a 2FA code sent to your phone. Far-fetched, I know, but sophisticated attacks often sound that way. I don't recommend automatically changing your email account's password in response to receiving an unsolicited 2FA code, but consider it a warning to be alert for additional indications of having been hacked.

- Accidental or random triggering: If you have a common email address or phone number, someone could have accidentally entered your address or number instead of theirs while trying to create an account. It's easy to type samuel45@example.com instead of samuel54@example.com or mistake the upstate New York 607 area code for the Boston 617 area code (a college friend at Cornell who grew up near Boston was once able to explain a wrong number call she received from someone attempting to call MIT, which used the same exchange as Cornell at the time). If you don't have an account at the site in question and receive only a single authentication code, you can probably ignore it. But again, stay alert for other issues.

- Glitches: There's no way to know if human or computer error was responsible for a 2FA code being sent out incorrectly, but stuff happens.

Regardless of the cause, if you ever receive an unsolicited 2FA code for a site where you have an account, change the password immediately. It's easy to do, particularly if you use a password manager, and the extra peace of mind is worth the effort.

By Adam Engst

14 Compelling Features Coming to Apple's Operating Systems in 2024

Apple's WWDC 2024 keynote was even more rapid-fire than usual, so much so that an Assassin's Creed game demo was the most relaxing part after the initial 90-second skydiving gag. It's tough—Apple presentations typically focus on a hardware product or three, but because WWDC is all about software, the company has to figure out which of the many new features merit a mention or demo. All too often, the presenter would introduce a feature, talk about it for a few seconds, and then switch gears entirely, just as I expected more detail or another feature in the same app.

In part, Apple's hurry came from trying to get through six different platforms before devoting a hefty chunk of time to Apple Intelligence, the company's name for a collection of AI features that will be rolling out over the next year. Apple said Apple Intelligence features would start being available "this summer," which probably means during the public betas of the operating systems starting in July, and would be broadly available in beta "this fall," or likely mid-September. However, Apple's footnotes acknowledged that "some features, software platforms, and additional languages will come over the course of the next year," probably well into 2025. Apple Intelligence will also require recent Apple silicon—it will run only on the iPhone 15 Pro, iPhone 15 Pro Max, and iPads and Macs with M1 or later chips. Apologies to our international friends, but Apple Intelligence will require Siri and the device language to be set to US English in the early releases. We'll look more deeply at Apple Intelligence in future articles.

Apple's six platforms now include macOS, iOS, iPadOS, watchOS, tvOS, and visionOS. Two notes: First, macOS 15 will be called Sequoia, which will undoubtedly become easier to type with practice. It's unclear if Apple meant to name it after Sequoia National Park or the iconic redwoods. Second, although Apple briefly talked about tvOS, the "platform" in question was called "Audio & Home" and seemed to encompass AirPods, HomeKit, and more. There was no mention of the HomePod.

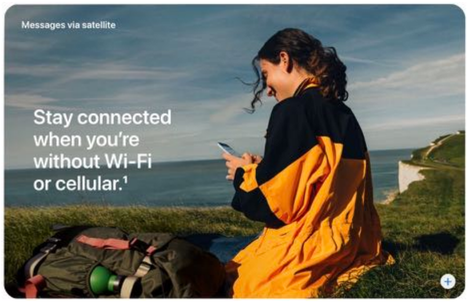
I couldn’t cover all the features Apple highlighted in the keynote, much less the many others it describes in preview pages on its website. Instead, I focus here on the features I look forward to trying or find generally compelling, in no particular order. For lists of everything coming in 2024’s operating systems—and Apple’s descriptions of the features below—see Apple’s preview pages for:

- macOS 15 Sequoia
- iOS 18
- iPadOS 18
- watchOS 11
- visionOS 2
- tvOS 18

All these operating systems are now available in beta form for developers, will appear in public beta form for everyone soon enough, and should ship in the usual September/October time frame.

Messages via Satellite

First in “Testing Emergency SOS and Find My via Satellite” (21 November 2022) and then in “Five Unexpected Announcements from Apple’s Wonderlust Event” (12 September 2023), I suggested Apple should allow sending location via satellite in Messages. The company went one better, providing Messages via satellite, linked to the existing iMessage and SMS networks. Conversations are end-to-end encrypted. The feature works only on the iPhone 14 and later, of course, and Apple said nothing more about charging for it, meaning that it’s still free through at least November 2025 (see “Apple Extends Free Emergency SOS via Satellite for iPhone 14 Users for Another Year,” 15 November 2023). I will be curious to see how well Messages via satellite works when both iPhones have no cellular service, as happens for me relatively frequently while working on trail races.



Siri Gets a Brain

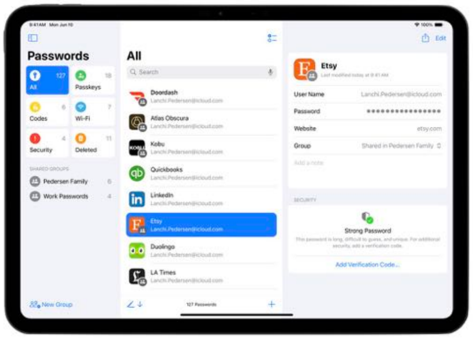
Most of what Apple shared about Apple Intelligence was relatively vague hand waving. But we all know and love/hate Siri. Like the Scarecrow in The Wizard of Oz, Apple Intelligence will give Siri a brain. Or at least that’s the promise, but I have high hopes because large language models are so much better than the token-based albatross of an architecture that has long dragged Siri down. Tonya and I rely heavily on Siri after going all-in on HomeKit—see “HomeKit for the Holidays (And Home Troubleshooting Tips)” (15 January 2021) and “Reflections on a Year with HomeKit” (17 December 2021)—and we’ve found Siri’s responsiveness and accuracy getting worse with time. If we say, “Siri, it’s time for dinner,” our Dinner scene usually triggers, but if we slip up and say, “Siri, it’s time to eat dinner,” we get restaurant recommendations. Apple promises that Siri will let us speak more naturally and understand us even if we make mistakes. My main worry is that because Apple Intelligence requires an A17 Pro or M-series chip on an iPhone, iPad, or Mac, Siri on the HomePod will remain as dumb as before.

Break Free of the Home Screen Grid

In iOS 18 and iPadOS 18, you’ll be able to customize the Home Screen far more than in the past. Previously, you couldn’t leave blank spaces between icons, but now you can arrange icons and widgets however you like, perhaps to allow your Home Screen wallpaper to shine through. Plus, you'll be able to change the size of icons and widgets, and even apply color tints. I can't tell if you can color icons separately or if they all (on a particular screen?) have to take on the same coloration, but we'll find out soon enough.

Passwords Becomes a Real App

It's about time. Over the past few years, Apple has been beefing up its built-in password management features, but to work with your saved credentials, you had to wade through the morass of Settings/ System Settings or Safari's settings. In iOS 18, iPadOS 18, and Sequoia, Apple has finally given us a standalone Passwords app. If nothing else, it will let us stop tripping over the iCloud Keychain and iCloud Passwords terminology and just call it Passwords. As I wrote in "[Using Apple's iCloud Passwords Outside Safari]" (1 April 2024), Apple's password management features are well above the bar, even if they aren't as complete as something like 1Password.



Etsy

User Name Lanchi.Pedersen@icloud.com

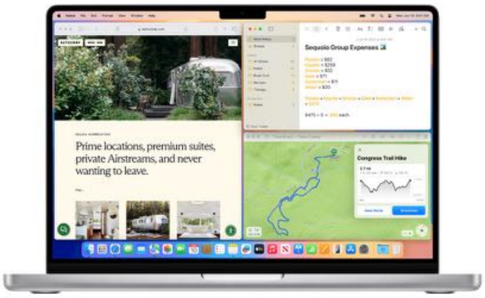
Password ••••••••••••••••

Website etsy.com

Group Shared in Pedersen Family

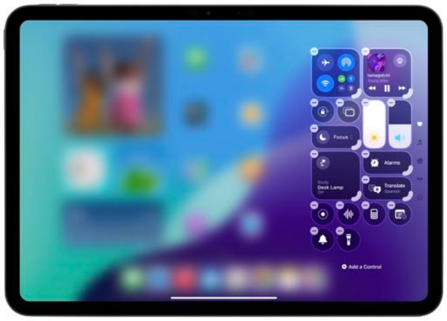
Automatic Window Tiling in Sequoia

In Sequoia, when you drag a window to the edge of the screen, it will offer to tile the window intelligently, suggesting a size and position that makes sense for the content. It could be a wonderful way to maximize the usage of your screen real estate. With this feature, Apple is Sherlocking an entire category of utilities, like Amethyst, BetterTouchTool, Magnet, Moom, Rectangle, and Yabai, but I gather that everyone has different and firmly held opinions on exactly how window tiling should work. So, if you like the idea of window tiling, you have lots of choices. Personally, I've found that having two 27-inch screens and keeping my apps in the same positions most of the time meets most of my needs, so I'll be curious to see if I find Apple's tiling helpful.


Prime locations, premium suites, private Airstreams, and never wanting to leave.
Sequoia Group Expenses
Congress Trail Hike

Control Center Construction Kit

Apple has overhauled Control Center in iOS 18 and iPadOS 18. It features groups of controls you can access with a single, continuous swipe down on the Home Screen. Along with the familiar Control Center controls, Apple showed a media player and a collection of Home tiles, and you can create your own groups. The new Controls gallery displays all the possible controls in one place, now including controls added by third-party apps, and you can mix and match them any way you want, even resizing them. It's hard to visualize exactly how this will work, but once Control Center reflects what you want, it may become a significantly more important aspect of the iPhone and iPad experience.



Mirror Your iPhone on Your Mac

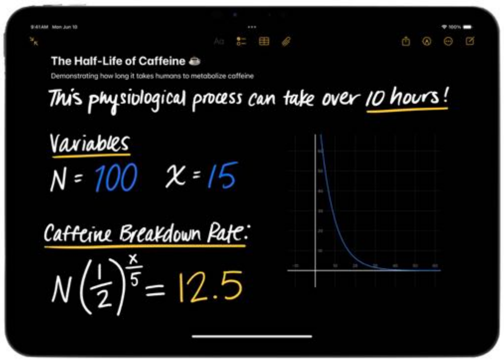
Do you find yourself regularly digging your iPhone out of your pocket even when you're working at your Mac? If so, you might appreciate the new Continuity feature that mirrors your iPhone in a window on your Mac. You can interact with the mirrored iPhone window as you would the actual iPhone, with your Mac's pointing device and keyboard working inside the iPhone interface. Audio from the iPhone comes through the Mac, and you can even share data between the Mac and iPhone using drag and drop. While the iPhone is being shared, it remains on its Lock screen or in StandBy. iPhone mirroring will require a Mac with Apple silicon or an Intel-based Mac with a T2 chip, along with the usual Continuity requirements with regard to Apple ID, Bluetooth and Wi-Fi, and proximity. A similar Continuity feature lets you get iPhone notifications on your Mac, and if you're mirroring your iPhone, click them to open the associated iPhone app.

visionOS 2 Gains Panoramic Mac Virtual Display

One disappointment of the initial release of Vision Pro was that it was limited to a single 4K virtual Mac display. Yes, you could put additional visionOS apps around the Mac display to increase the information density of your environment, but it couldn't simulate a Mac with two displays. visionOS 2 promises an expandable, ultrawide, wraparound screen that provides the equivalent of two 4K displays side-by-side. It falls into the "coming later this year" category and sounds like it will work only with a Mac running Sequoia.

Math Notes in the iPad's New Calculator App

In another "about time" feature, Apple has finally brought the Calculator app to the iPad, refactoring it for the iPad's larger screen. But Apple didn't stop there, adding history and unit conversion to both versions. The most compelling addition is Math Notes, which demos best on an iPad with an Apple Pencil. You can handwrite equations, and as soon as you draw an equals sign, Calculator solves the equation. It supports variables, and if you edit an equation, the results change on the fly. (Sorry, Soulver!) You can even add graphs. I doubt I'll use Math Notes because I switch to a real spreadsheet when I have to go beyond simple math. However, I can see students relying heavily on the feature as they explore the mathematical underpinnings of various academic disciplines. Math Notes is also available within the Notes app, and that appears to be the only way you can use it on a Mac.



The Half-Life of Caffeine

Demonstrating how long it takes humans to metabolize caffeine

This physiological process can take over 10 hours!

Variables

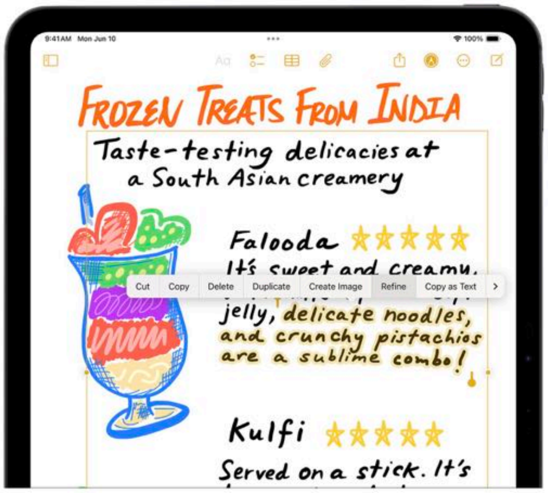
$N = 100$ $x = 15$

Caffeine Breakdown Rate:

$N\left(\frac{1}{2}\right)^{\frac{x}{5}} = 12.5$

Smart Script Improves Handwriting

While we're on the topic of the Apple Pencil, iPadOS 18 will provide Smart Script, which improves the appearance of your handwriting as you write, making your lettering smoother, straighter, and more readable while maintaining your handwriting style. You can even paste text in and have it look like you wrote it. Spell checking fixes mistakes inline, and scratching out text with the Apple Pencil erases it. My handwriting is mediocre at best, and one of my irritations with the Apple Pencil was that what I wrote wasn't all that legible—perhaps Smart Script would help. Realistically, handwriting is too slow—I'll always revert to typing when taking notes.



FROZEN TREATS FROM INDIA

Taste-testing delicacies at a South Asian creamery

Falooda ★★★★★

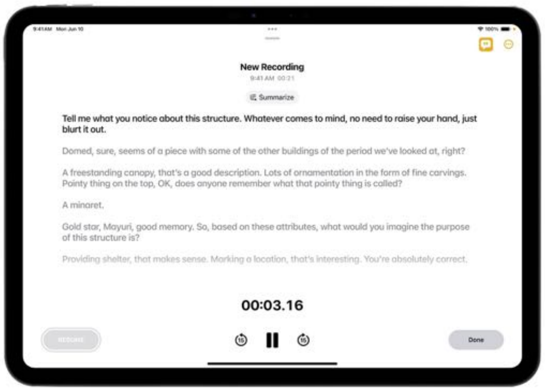
It's sweet and creamy, ... jelly, delicate noodles, and crunchy pistachios are a sublime combo!

Kulfi ★★★★

Served on a stick. It's

Notes Gains Audio Recording and Transcription

Here's a feature I'll use in every talk I attend from now on. The Notes app on all platforms will record audio and create live transcriptions. In fact, for Apple's WWDC keynote, I set up Rogue Ameoba's Audio Hijack to record and transcribe the audio. It did a fine job, and I searched through the transcript several times while writing this article to remind myself of specific quotes. You'll notice a Summarize button in the iPad screenshot below, and while I tried to feed all 88 KB of the WWDC keynote transcription to various free chatbots for summary, only Claude and Perplexity took it. In neither case was the summary particularly helpful because Apple's keynote script was already so concise, so the summary ended up skipping most things. Claude did a much better job when I asked it to list all the features, categorized by operating system. We'll see how helpful Apple's summarization is, but transcription alone is a big win. I hope the feature doesn't cut into Rogue Amoeba's market too much, but I assume few Audio Hijack users use it solely for its transcription capabilities.



New Recording

9:41 AM 00:21

Tell me what you notice about this structure. Whatever comes to mind, no need to raise your hand, just blurt it out.

Domed, sure, seems of a piece with some of the other buildings of the period we've looked at, right?

A freestanding canopy, that's a good description. Lots of ornamentation in the form of fine carvings. Pointy thing on the top, OK, does anyone remember what that pointy thing is called?

A minaret.

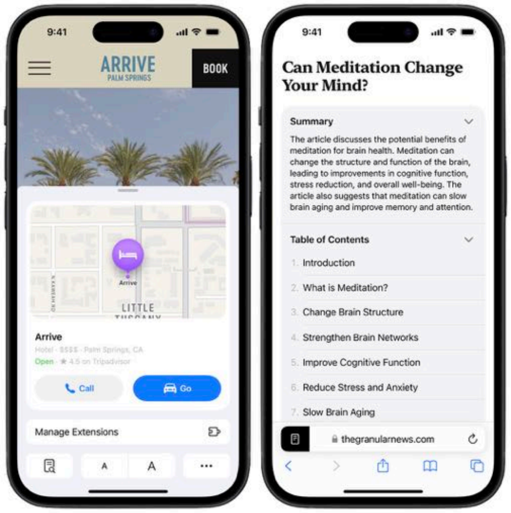
Gold star, Mayuri, good memory. So, based on these attributes, what would you imagine the purpose of this structure is?

Providing shelter, that makes sense. Marking a location, that's interesting. You're absolutely correct.

00:03.16

AI Provides Safari Highlights and Reader Summaries

Although these features aren't enough to tempt me away from Arc and Arc Search, devoted Safari users might find them helpful. Using AI, Safari's Highlights feature will automatically detect and display relevant information on a page—directions, biographical information, and details about popular media. No more searching for the address just to get directions to a restaurant. Plus, Safari uses AI to generate a table of contents and high-level summary for articles you add to Safari Reader.



Arrive

Hotel · $$$$ · Palm Springs, CA

Open · ★ 4.5 on Tripadvisor

Can Meditation Change Your Mind?

Summary

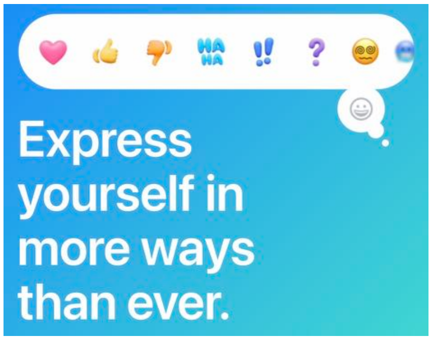
The article discusses the potential benefits of meditation for brain health. Meditation can change the structure and function of the brain, leading to improvements in cognitive function, stress reduction, and overall well-being. The article also suggests that meditation can slow brain aging and improve memory and attention.

Table of Contents

1. Introduction
2. What is Meditation?
3. Change Brain Structure
4. Strengthen Brain Networks
5. Improve Cognitive Function
6. Reduce Stress and Anxiety
7. Slow Brain Aging

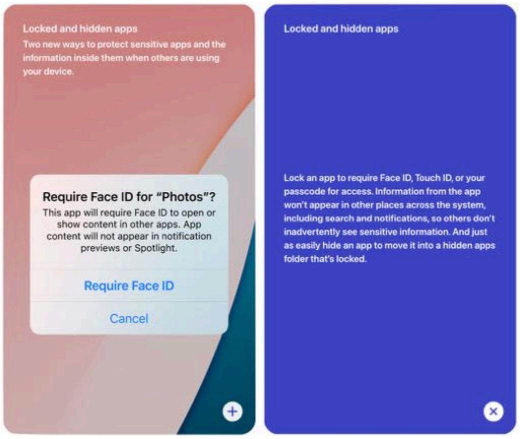
Tapbacks Get Funky

I'm fond of tapbacks, the little icons you can use in Messages to respond subtextually. Currently, we're limited to a heart, thumbs up and down, laughter, exclamation points, and a question mark. Those cover a lot of instances of "Your message evoked an emotion, but I don't have anything else to say," but in the next set of operating systems, you'll be able to use any emoji or sticker for a tapback response. Eventually, with Apple Intelligence, you'll be able to create Genmoji with textual descriptions ("a penguin wearing sunglasses") and use them anywhere you use emoji, including in tapbacks. Messages will also allow text formatting (bold, italic, and underline) and provide text effects that look about as cheesy as gestural reactions in video.



Lock and Hide iPhone Apps

We've all got something to hide. When you hand your iPhone to a friend to look at a photo or read a Web page, you probably don't want them poking around further. New privacy features in iOS 18 and iPadOS 18 will let you lock apps so they require Face ID or Touch ID for access, and information from them won't show up in search results or notifications. You can also move apps to a hidden folder in the App Library that can't be opened without Face ID or Touch ID.



Locked and hidden apps

Two new ways to protect sensitive apps and the information inside them when others are using your device.

Require Face ID for "Photos"?

This app will require Face ID to open or show content in other apps. App content will not appear in notification previews or Spotlight.

Locked and hidden apps

Lock an app to require Face ID, Touch ID, or your passcode for access. Information from the app won't appear in other places across the system, including search and notifications, so others don't inadvertently see sensitive information. And just as easily hide an app to move it into a hidden apps folder that's locked.