

printout

Keystone MacCentral Macintosh Users Group ♦ www.keystonemac.com

Keystone MacCentral May Program

May 17, 2022 07:00 PM

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

This month we plan to have presentations on

Apple ID Account Recovery Methods

*Of particular interest this month
as Linda is attempting to recover an account
for an acquaintance whose iPhone went missing*

And

**Understanding How to Format Your New External Hard Drive
– A Look at Apple's Disk Utility**



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 May Program	1
Apple's App Store Stubbornness May Be iOS's Greatest Security Vulnerability <i>By Rich Mogull</i>.....	3 - 9
Use the Web to Cook Your Books <i>By Jeff Carlson</i>.....	9- 13
Using Universal Control in macOS 12.3 Monterey and iPadOS 15.4 <i>By Josh Centers</i>.....	13 -18

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 © 2022, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles from 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.

Board of Directors

President

Linda J Cober

Recorder

Wendy Adams

Treasurer

Tim Sullivan

Program Director

Dennis McMahon

Membership Chair

Eric Adams

Correspondence Secretary

Sandra Cober

Newsletter Editor

Tim Sullivan

Industry Liaison

Eric Adams

Web Master

Tom Bank II

By Rich Mogull

Apple's App Store Stubbornness May Be iOS's Greatest Security Vulnerability

When Apple decided to support applications on the iPhone in 2008, it did so in the most Apple way possible (see "[Apple Announces iPhone 2.0, Releases SDK](#)," 6 March 2008). The company distilled the complex process of finding, purchasing, downloading, and installing apps down to a simplified user experience. With the App Store, customers could go to a single storefront and do everything with the tap of a finger. Apple vetted apps to meet the company's standards and security requirements, providing customers both convenience and peace of mind.

Apple prioritized iOS security from the start, realizing that customers were more likely to buy iPhones and apps if they didn't have to worry about malware. The company leveraged its complete control of iPhone and iPad hardware, iOS, and the App Store to create one of the most secure software ecosystems in the history of personal computing, rivaled only by gaming consoles. Perfect? No. Highly effective? Absolutely. Apple built a security model based on *vertically integrated security* that combines hardware, software, and services, with the App Store playing a key role (see "[Apple Platform Security Guide Reveals Focus on Vertical Integration](#)," 18 February 2021).

But this foundation is now at risk, largely due to how Apple has treated app developers and payments. On 25 March 2022, [the European Union published its draft Digital Markets Act](#). If enacted, the legislation would, among other things, require Apple and similar companies to support alternative app stores. [Apple is still embroiled in a lawsuit with Epic Games](#) that focused on forcing non-Apple app stores onto iOS. Over in the Netherlands, Apple has been [forced to open up external payment systems](#) for, of all things, dating apps. While supporting alternate payment systems doesn't affect security,

opening up to alternative app stores will have profound implications.

Apple largely has itself to blame. Apple didn't create a walled garden marketplace merely to ensure consumer safety; it also did so to own the billing model and financial transactions, and thus the customer relationship. Until a week ago, a developer wasn't even allowed to link to or mention their website for prospects to sign up for subscriptions. For over 13 years, Apple refused to budge to pressure from developers, forcing them to turn to the courts and legislatures.

Let's distill this down to understand why the App Store is so important for security, how opening iOS up to alternative app stores or sideloading will reduce our safety, and why this now seems inevitable.

How does the App Store work with iOS security?

Apple uses a *vertically integrated* security model for iOS devices. That means that the overall platform security is provided by Apple hardware, software, and services all working together. You can read the details in the [Apple Platform Security Guide](#), but here is a simplified summary:

- Developers write their app code using Apple's tools, which automatically enable certain security features to reduce the risk of vulnerabilities.
- To submit apps, a developer must be approved by Apple and issued a digital certificate to sign their apps. Apple tries to validate that the business is real, but experience tells us that it doesn't always get it right.
- Developers sign their apps and submit them for approval. Apple assesses each version of each

app, including running security scanners to find common coding vulnerabilities.

- By default, apps are completely isolated and have no access to user data anywhere on the device. Even access to capabilities like Bluetooth is restricted. Developers who want additional access must request an *entitlement* from Apple.
- If approved, the application and its entitlements are cryptographically signed by Apple and placed on the App Store. I'll explain why this is so important in just a moment.
- On the device side, iOS boots up using a *chain of trust*. This complex process relies on a series of digital signatures and code signing checks to assure that each part of the operating system is official, trusted, and tamper-proof. It also relies heavily on the *Secure Enclave*, which manages cryptography functions and holds the root encryption keys and certificates in a secure portion of the device's system-on-a-chip so they can't be modified.
- When an app runs, the operating system extends the chain of trust to the certificate used to sign the app itself. That certificate must be valid, and the app's code has to match code signature checks that ensure it hasn't been modified since it was installed or updated.
- Part of this process validates the app's entitlements. Apple signs those so an app can't suddenly start reading your contacts if it hasn't officially been approved for an entitlement. Many entitlements also won't work unless the user is prompted and approves the access. Facebook can ask to see your contacts, but you don't have to let it. (And for the sake of the privacy of all your contacts, don't!)
- The app then runs in a sandbox that is isolated from the rest of the software on the device. Apps are provided their own file storage, separate from other apps. iOS uses internal security capabilities to enforce this isolation. When apps do need access to shared resources or each other, this access is also controlled by

iOS and relies (partially) on more digital signatures for enforcement.

Now explain it like I'm a fifth grader?

Sure thing. Apple scans every app submitted to the App Store for malware and security vulnerabilities. After approving an app, Apple puts it in a digital envelope sealed with digital wax (those signatures and certificates we talked about). Hardware and software on our iPhones and iPads check the seal and ensure the app was approved and no one has tampered with it. That same hardware and software then isolate the app when it runs so it can't do bad things. All this keeps your device safe and, via entitlements, protects your privacy.

The entire system relies on Apple services (the App Store and developer program, plus digital certificate servers), Apple software (iOS and iPadOS), and Apple hardware (the Secure Enclave and certain other hardware protections we are skipping).

This sounds great, so malware is impossible on iOS?

Alas, no. There has been malware on iOS. It's just a lot harder and more expensive to create, much more difficult to distribute, and far easier to shut down. For example, [the NSO Group developed an incredibly sophisticated iOS exploit](#) that relied on building a Turing-complete emulator within an obscure PDF feature.

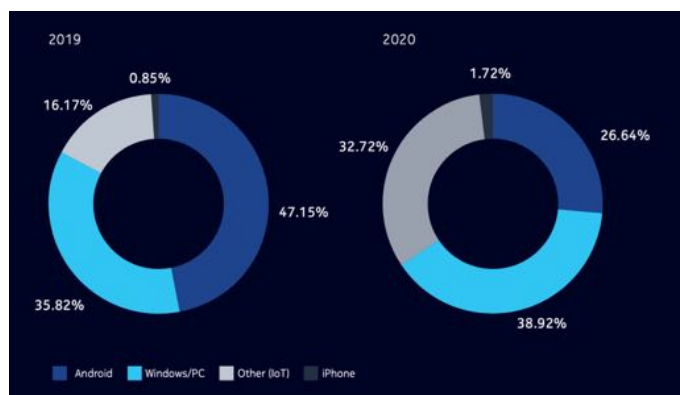
There are also plenty of scammy apps in the App Store that meet all of Apple's security requirements but still come up with ways to trick users out of their money through sneaky subscriptions or by targeting kids. Unpleasant as these apps are, they can't take over your iPhone and spread to other devices on the same network.

How do we know this all actually works?

As we like to say in the security world, the proof is in the pudding. There has never been any widespread malware on iOS. [Malware is more of an issue on Android](#), but even there it is less of a

concern when users stick with the official Google Play Store.

In Nokia's [Threat Intelligence Report 2020](#), the company shared a breakdown of malware infections by device for 2019 and 2020. In 2019, Android led with 47% of infections, compared to less than 1% for iOS (the other two categories were Windows PCs at 36% and Internet-of-Things devices at 16%). However, noting that the security of official app stores like the Google Play Store has increased continuously, Nokia found in 2020 that Android accounted for only 27% of infections, and iOS remained under 2%. (Windows increased slightly to 39%; the IoT devices drew most of the malware attention, jumping to 33% of infections.)



Source: Nokia

These numbers support the fact that there is vastly less malware targeting iOS than Android, thanks to Apple's insistence on a single App Store. Even within the Android world, the increasing security of the Google Play Store resulted in an overall drop in malware infections, even though they remain high due to the availability of alternative app stores and sideloading.

Why are digital signatures so important?

Earlier, I mentioned the chain of trust. Many forms of malware find a vulnerability on a computer and then use that to embed themselves in some pre-existing piece of software. This technique enables attackers to establish persistence, so the malware doesn't just run in memory and disappear when the app shuts down or you reboot.

The chain of trust does two things. First, it uses cryptographic signatures to ensure the running software comes from a trusted source. That's why Apple embeds a read-only signature onto its devices; the attackers have no way to swap in a different signature to fool your iPhone into thinking that it's running trusted code. Web browser developers like Google do something similar by embedding known signatures into their browsers as certificates that enable a "root of trust." These root certificates are trusted by the Web browser companies and are used to sign and validate the site-specific certificates used by websites, so you get those little green validation marks when you connect to your bank.

For apps, Apple also makes a cryptographic "hash" of the code and signs it digitally. A hash is a manageable number that maps to the app's code and changes if even a single bit of the code changes. iOS can then ask, "Does this app come from where I expect?" and "Did the app change at all?" (And obviously, if the answer to either of those questions is "No!" iOS won't let the app run.)

On iOS, this chain of trust runs from the lowest levels of the operating system when our iPhones and iPads boot, all the way to the apps we download and run from the App Store. The entire chain relies on these digital signatures, certificates, and hashes.

Tell me again how knowing all this improves security?

There are three benefits:

- We know that all apps in the App Store have been scanned and approved by Apple. This significantly reduces the risk that an app we download is deliberately malicious or accidentally harmful.
- We know that all the apps on our iPhones or iPads came from the App Store and are running the same code that we downloaded—malware infections that modify apps are nearly impossible.

- We know that apps can't get—or even ask for—access to data like contacts or calendars, or features like Bluetooth, without Apple having approved their entitlements.

What about sideloading?

Sideloading means allowing users to install apps directly, without going through any app store. Typically, users must enable sideloading manually, since devices default to staying locked down, but it's still a huge security hole. Alternative app stores enable installing apps from additional, hopefully trusted sources. Sideloading lets users install anything they want... or can be tricked into installing.

Of course, sideloading is nothing new—it's how things work on the Mac today, where you can install any app from any source. Although much Mac malware takes advantage of sideloading, none of it has been truly widespread so far. That's more likely a side effect of the Mac being a relatively small target; there are so many more iPhones and iPads combined that malware authors target them even though it's very difficult; if it got easier, we'd see many more attacks.

Could Apple enable alternative app stores?

Yes. There are two ways Apple could support third-party stores:

- Apple could authorize another store and issue it a certificate with which it could sign its own apps, after which the chain of trust would expand to include that certificate. This approach would be similar to how Web browsers come bundled with a series of root certificates used to sign the certificates of websites, although [that system has been abused as well](#).
- Apple could also issue certificates to all comers or disable some or all of its existing security checks for apps that users download from a third-party store. This approach, which is how things work on Android, would make possible a range of potential app stores with widely

varying approval policies and levels of security.

Why do alternative app stores reduce security?

It comes down to consistency and enforcement. Apple couldn't review the apps in those stores and ensure they meet Apple's requirements. Nor would Apple be able to review entitlements in those stores. The alternative app stores would only be as secure as they want to be and are capable of enforcing.

If Apple were to allow only a small number of vetted alternative app stores, this might not be too terrible. Apple could set standards for those partners and issue them special certificates to sign their own apps. Then Apple could build a security program to ensure those partners met and maintained standards that were at least equal to Apple's.

On the other hand, if Apple were required to allow any arbitrary alternative app store, we immediately run afoul of the same problems that plague Android since there is no way to enforce any security standard. This model would either require Apple to issue certificates to anyone or, more simply, enable users to disable the signing mechanisms and allow any app to run without the security checks.

The first option is much more secure, but it doesn't provide many benefits to the third-party app stores beyond handling their own payments (I'll get back to that). Also, Apple would likely still draw complaints similar to those the company faces over the official App Store, since Apple would have to set standards to be in the program, charge to participate, and probably anger all sorts of alternative app stores that don't align with Apple's goals. The second option creates a free-for-all without any security enforcement, and we can already see how that model results in a less-secure, malware-friendly environment on Android.

Couldn't users just stay secure on the official Apple App Store?

Users could choose to trust only Apple, but over time, there would be both direct pressure and scams to move users to alternative app stores. Some popular apps might require you to use an alternative app store and decline to participate in Apple's. Most people aren't computer security experts and won't know the implications of trusting a new app store on their phones, and even tech-savvy users will be forced to install Facebook, Instagram, and WhatsApp.

What if your bank only supports an alternative store? Or someone tricks you into thinking your bank only supports an alternative store? How certain are you that you'll be able to make the safe decision every time one comes up? Alternative stores and sideloading increase security complexity for users, and history shows us that complexity opens up opportunities for attackers.

Again, we already see this on Android, where users can be tricked into sideloading or using an alternative, untrusted app store to install some app without realizing it is a scam or malware.

Isn't this how "enterprise applications" work?

Apple does have a program for enterprises to build and install their own apps onto corporate-owned devices. This is exactly how the best-case alternative app store model could work. Apple issues a certificate to these companies, which then use a process to install the certificate on employees' iPhones, allowing apps signed by that company to run.

[This system was abused by Facebook](#) a few years ago, which highlights the trust issues that come into play when Apple starts handing out certificates.

Don't gaming consoles do the same thing?

Absolutely. Apple didn't invent the app store model or create the first walled garden marketplace. Video game consoles are probably the closest example. They are powerful computer systems with single-source app stores and locked-down hardware. Game companies have been

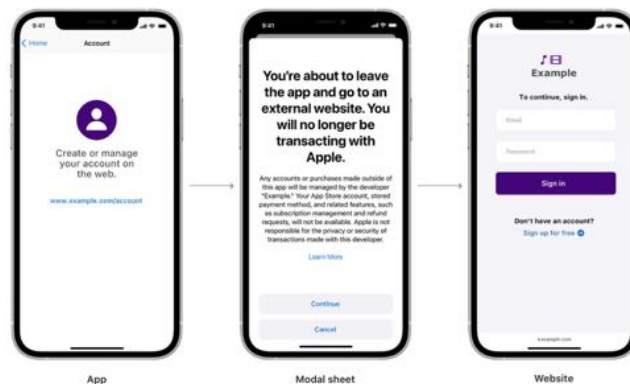
running walled garden marketplaces since the first home systems appeared. The only difference back then was that we only loaded games from physical media, like cartridges or CD-ROMs.

As a result, game systems also have extremely low rates of malware and scams, just like the iOS ecosystem.

Why do developers and companies want alternative app stores?

The first answer is easy: "follow the money." Right now, Apple enforces app standards (such as no "adult" apps) and takes a 30% cut of all sales made within apps (there is now some variation in the fees). Apple also takes a cut of all in-app purchases. This is why you haven't been able to buy a new book in the Kindle app; Amazon doesn't want to pay Apple 30% of every book sale when it can instead make users buy books within their Web browsers and not share any of the revenue with Apple.

The problem is that Apple has also long prevented Amazon and other companies from linking out to their websites for purchases or even telling users that it's an option. Happily, after pressure from Japan and the Netherlands, [Apple has relaxed its rules](#) to allow alternative payment options or linking to external subscription services. "Reader apps" that are primarily meant to provide access to digital content, such as Kindle, Netflix, Spotify, and others, can now direct users to an external site for payment, albeit with some rather stiff required language. (At least it's better than it used to be.)



Source: Apple

Apple does deserve some cut of transactions—running the App Store does entail significant costs—but well below the standard 30%.

Apple also has a history of frustrating developers in other ways. It sometimes rejects apps for seemingly arbitrary reasons. It doesn't do a good job blocking clones and copies of popular apps, which can damage small developers. It puts in obnoxious requirements, like requiring developers to use "Sign in with Apple" if they also enable "Sign in with Google" or any other third-party sign-in service. Plus, there are entire categories of apps Apple simply doesn't want on its platform and won't accept into the App Store.

Regardless, money, more than frustration, is what drives the push for alternative app stores. I highly doubt Epic Games is suing Apple for any reason other than the cash. It just so happens that Epic Games has its own app store for games where it takes a cut of all the sales from the developers in its ecosystem. Just like Apple does now. And no, the Epic Games Store doesn't allow alternative stores within it, either.

Money comes into play in another way, too: privacy. Some developers and payment providers want to track users and their purchases so they can further monetize this information. Right now, Apple owns the customer relationship for in-app purchases, which is why, for example, you aren't spammed by every app you ever downloaded. If you don't create an account with a particular developer, they have no idea who you are. Also, if you sign up for a subscription to something in the App Store, it appears on your account and you can cancel whenever you want without having to jump through any hoops.

In short, Apple enforces its philosophy that you are the customer, not the product being sold. There are robust ecosystems to track and sell your data that are significantly more restricted on iOS than Android because of Apple's requirements. For example, [Facebook is losing billions of dollars](#) because Apple now forces the Facebook app to ask users for permission to track them. Well, and because [96% of users in the US opt out](#) when asked.

Why are regulators forcing Apple to support alternative app stores?

Many companies have been unhappy with the App Store's restrictions and financial model. Some of these companies, like Epic Games, have sued Apple in an attempt to force changes via the courts, while others have been lobbying governments. Apple is a huge target, and the European Union, in particular, is open to using regional regulations to increase the competitiveness of its local businesses by forcing interoperability.

Global technology companies like Apple, Google, and Meta (Facebook) are facing increasing scrutiny worldwide due to their dominance across society. Issues surrounding alternative app stores and sideloading are among the many regulatory questions surrounding the tech giants, along with antitrust investigations, encryption regulations, and complex issues around content moderation and [ownership](#).

From one perspective, it seems unfair to force Apple to allow alternative app stores, given that it built a completely contained robust marketplace in a world with Android's even larger competitive ecosystem.

The opposing view recognizes that mobile devices have become essential and ubiquitous—in the future, everyday activities will be more difficult or even impossible without one. (In some places, you now need a smartphone to scan a QR code at a restaurant even to see a menu.) That points toward governments wanting some say in how their citizens are treated. The world is dominated by just two platforms, Apple and Google, both of which rely on their own app stores ([Google also takes a 30% cut](#)), but only Apple's is mandatory.

Right now, the European Union is the biggest threat to Apple's model because of its sheer size and influence. But we also see lawsuits and [proposed regulations here in the United States](#), including the Epic vs. Apple case, which is on appeal. (Full disclosure: I signed an amicus brief to the courts in that case highlighting the dangers of alternative app stores.)

Couldn't Apple just allow alternative payment systems and keep the App Store secure?

It may be too late to prevent governments—or possibly the courts—from forcing Apple to support alternative app stores and maybe even sideloading. Apple had many years to respond to the complaints and concerns that led companies to file lawsuits and lobby lawmakers. When Apple talks about keeping the App Store locked down and exclusive, it always focuses on security without acknowledging the financial side of the equation.

I believe that Apple could have reduced the likelihood of being forced to accept alternative app stores and sideloading by decoupling the security of the App Store from payments. Apple continues to fail to discuss or even consider App Store payments separately from App Store security, but the two are only slightly related. (Apple has some legitimate concern in preventing customers from being scammed by alternative payment systems, but that's largely unrelated to platform security.) I can't help but think that developer complaints would have been far more muted had Apple loosened some of its payment restrictions and percentages more aggressively. Apple might not be in this position today if it has been more responsive to developers in the past.

Courts and regulators aren't technology experts and seldom understand subtleties like the difference between payments and security. They tend to use a sledgehammer instead of a screwdriver. Apple simply let App Store dissatisfaction simmer for too long.

What will happen now?

Sadly, from my perspective as a security expert, I think that courts and regulators will force Apple to support both alternative app stores and sideloading within the next few years. This will materially increase the security risk on iOS devices, especially for those less familiar with technology who don't understand the security risks. It will start in Europe but quickly spread to other regions, including the US. It could also have larger implications in markets like China, where the government will likely try to exert even more control over what Chinese citizens can buy—imagine a highly regulated Great Bazaar to match China's Great Firewall.

As Apple customers, we can still protect ourselves. Personally, I plan to stick with Apple's official App Store and will continue to recommend the same to anyone willing to listen. I fully expect Apple to default to the same level of security we have today and require users to jump through a (hopefully) painful process to authorize other app stores and sideloading. I also fear that, at least at the start, the technical updates required to support alternative app stores will create new attack surfaces and security vulnerabilities that could have a broad impact.

If any lawmakers, regulators, or judges are reading, I implore you to explore the implications of such requirements and consider that there are options to force payment processing changes rather than blowing up the entire security model that has kept iPhones so safe for over a decade. 🍷

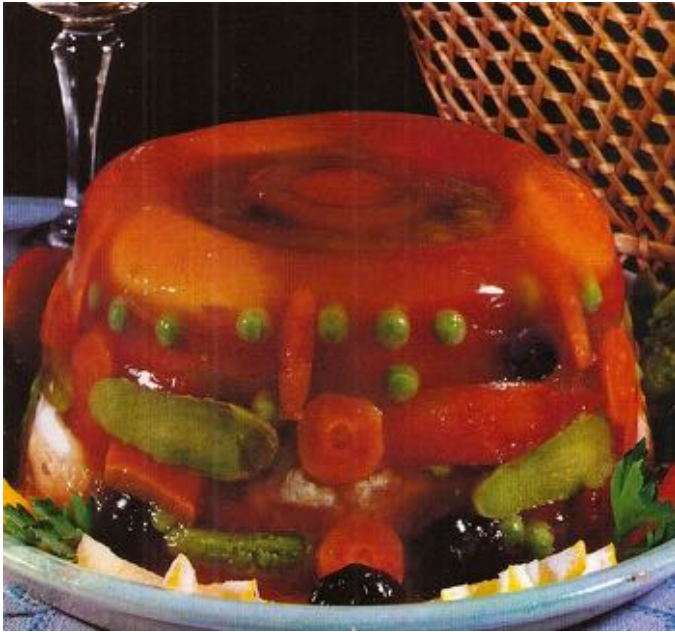
By Jeff Carlson

Use the Web to Cook Your Books

At some point during the last year, my teen declared that I wasn't allowed to buy any more cookbooks. We had run out of space in the kitchen, even after a culling session that weeded out some old titles ([exotic Jell-O recipes from the](#)

[middle of the last century](#) won't be coming back, nor am I likely to cook dinner for dozens). And let me reassure you, my collection is modest compared to many home cooks, maybe a few dozen titles in all.

You're not ready for my jelly, are you

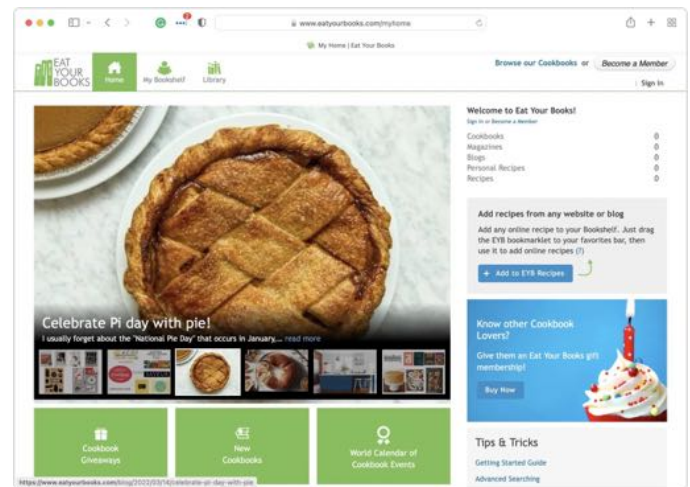


But I still run into the cookbook conundrum: finding a recipe involves keeping a mental model in my head of which books contain my favorite recipes, and when that fails, I have to flip through multiple volumes. Even though my library is small, the books are shoehorned into various available corners of my kitchen, so I also need to remember where each one is located. (And are they organized in a sensible fashion? No. Have you met me?)

So, like many people, I often turn to a Google search for recipes. That's fine—if often overwhelming—but it feels like I'm cheating on my cookbooks, which I purchased because they're beautiful, informative, and usually tell a story about the chefs or the cuisines they feature. I like cookbooks!

Then I discovered [Eat Your Books](http://www.eatyourbooks.com), a website that combines the searchability and discoverability of

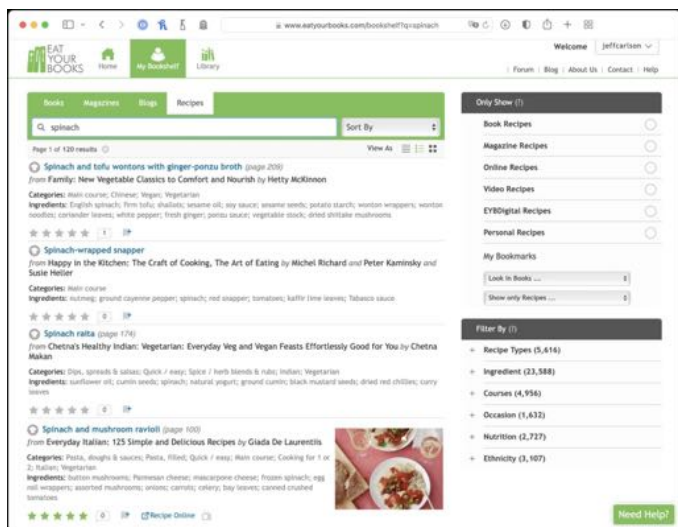
modern technology with the richness (and generally higher quality) of printed cookbooks.



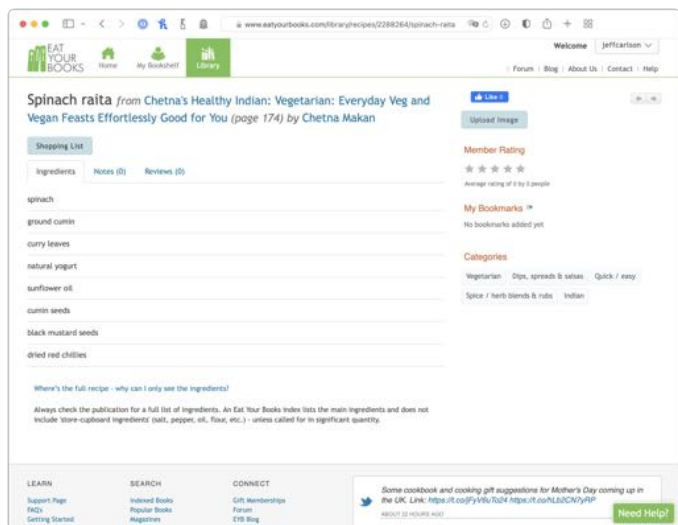
Disclosure: You Don't Eat Any Books

The core of Eat Your Books is an extensive reference database of the contents of over 160,000 cookbooks and food magazines. It won't show you any actual recipes because, the company says, that would violate copyrights. ([That's not precisely true](#); lists of ingredients and simple sets of instructions are not copyrightable. However, recipe introductions and creative instructions can be protected. I suspect the company is trying both to support authors and avoid potential litigation.) Instead, you can search for the name of a dish or ingredient and see matching recipes that come from the books you own.

For instance, let's say I have some spinach that I need to cook before it wilts. At Eat Your Books, I can click My Bookshelf > Recipes in the toolbar at the top, enter "spinach" in the search field, and view all the recipes in my cookbooks that include spinach. Since spinach is such a common ingredient, I can also filter the results, such as narrowing it down to just recipes from India.



When I click a recipe that looks good, Eat Your Books presents me with the cookbook and the page number on which it appears, along with a list of ingredients so I can make sure I have them all on hand. I can add the items to a simple Shopping List view that I can print or bring up in Safari on my iPhone when I'm at the store.



A free Eat Your Books account lets you add up to five books or magazines and an unlimited number of sources for online recipes. A Premium membership, which removes those limitations, costs \$3 per month or \$30 per year.

Adding a book to your library is speedy. Using the search field under Library > Books, I found nearly all of my cookbooks by typing just partial book titles. You can also enter an ISBN. I was going to

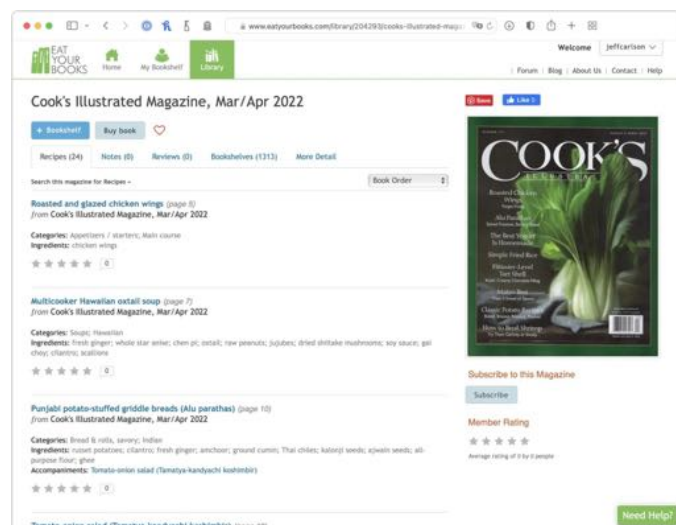
make a joke about how I've misplaced my [CueCat](#), and how it would be great to scan barcodes if you have a large library... and then I discovered that the [Import Books](#) feature does exactly that.

Seeing large book covers as icons is a huge help, such as when I needed to specify that I own the 1997 edition of *Joy of Cooking*, not earlier or later editions.

Not all of the books in the Eat Your Books library have been indexed. You can still add one to your bookshelf, but you won't see search results from it. This happens with "books that are unlikely to be indexed by EYB because they are not on sufficient [numbers of] Bookshelves." In that case, you can click the Request Index link and [ask Eat Your Books to add it to the indexing to-do list](#), or you can [request to index the book yourself](#).

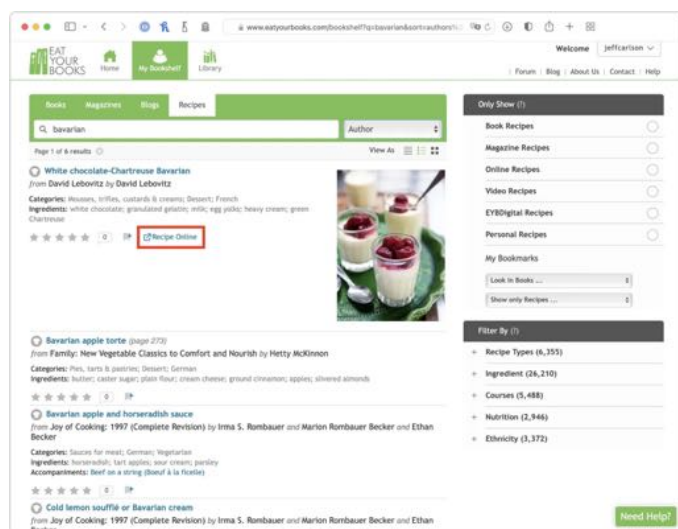
Side Dish Sources of Recipes

Books are the main course, but you can also add food magazines and blogs to your bookshelf. With magazines, you can add each issue as it becomes available or specify that you subscribe to the title to automatically add new issues as they are indexed. To catch up on your back issues, [enter a date range of issues](#). The format is the same: recipe names, ingredients, and page numbers for that issue.



Indexed blogs are in some ways the most interesting part of Eat Your Books because they include a Recipe Online link that takes you to the

actual recipe published on the site. Being able to search through a curated set of food blogs is a huge win. There must be hundreds of thousands of them (most telling you at length what Hubby and Precious Child think of their recipes before getting to the actual recipe), rendering the results from a general Google search overwhelming. With Eat Your Books, though, you can restrict your searches to the food bloggers whose taste and expertise you appreciate.



You can also add notes and reviews to recipes on your bookshelf, which can be shared with the greater Eat Your Books community or saved privately in your account. The public notes can be helpful to scan for recipes you haven't made before, though they still occasionally suffer from comments from people who made numerous radical substitutions but are peeved that the recipe didn't come out right. Of course, you can bookmark favorite recipes to aid in quickly getting back to them—or at least to their page numbers.

If you run across an online recipe you like, you can use a bookmarklet to add it to your bookshelf. It attempts to scrape the information from the site and pops up a window for you to add other information that wasn't grabbed. However, the recipe must be approved by Eat Your Books before it goes into the library. I've long used the service [AnyList](#) for saving recipes, which does a great job. Others at TidBITS are fond of Paprika (see

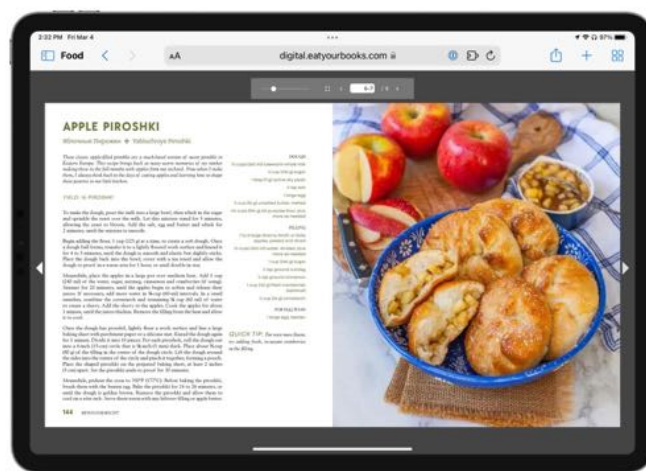
[“FunBITS: Paprika Recipe Manager for iPhone, iPad, and Mac,”](#) 14 March 2014).

Feed Your Cookbook Appetite

You can also browse for cookbooks you don't own. The Eat Your Books home page spotlights books, ingredients, and food-related news, such as a feature on cookbooks that celebrate the cuisine and people of Ukraine. Eat Your Books also features reviews of new titles and lists of best-selling titles from many independent booksellers, including my favorite local all-cookbook book store, Seattle's [Book Larder](#).

When you're browsing a cookbook, you can also see how many people have it in their bookshelves, which is a great way to see which titles are popular. The list also reveals how many books the members own—or at least have added to their bookshelves. It's not uncommon to see people with thousands of titles!

Some cookbooks in Eat Your Books include EYB Previews, which are PDF-like selections containing a few pages to give you a feel for the recipes and look. As you can see, the site also looks great on an iPad.



Unsurprisingly, if you find a book you want, you can buy it using affiliate links that support the site.

A Few Scorched Edges, but Overall a Good Bake

I have only a few criticisms of Eat Your Books. Some older recipes (pre-2015) don't include page numbers, only cookbook titles. That's not a major problem, since you can always check the table of contents or index when you actually open the book.


A trivial annoyance is navigation. It would be nice if the home page would display a search field for My Bookshelf > Recipes when you're logged in. But it's easy enough to create and use a bookmark to the My Bookshelf page, whose search field does default to Recipes.

These are minor gripes. Although Eat Your Books is a database at its center, its heart is the love of cookbooks shared by its members. The site is trying to make a cook's life easier and more integrated

with the real world, not supplant the beauty and storytelling qualities of good cookbooks. It also helps me get out of ruts where I cook the same handful of dishes from the few cookbooks I can remember and reach.

A Note Just In Case...

Great idea! But when I went to try it, first I got a "website not secure" warning that I had to override, and then "not found"...

The URL works if you put [www](#) in front of the URL. It worked fine during editing, so something must have broke on their end in the interim and we didn't think to test. It should be fixed now 

By Josh Centers

Using Universal Control in macOS 12.3 Monterey and iPadOS 15.4

Universal Control may be the most-delayed feature of Apple's 2021 operating systems, only just now appearing in macOS 12.3 Monterey and iPadOS 15.4, but it's one of the most interesting. Universal Control lets you use a single keyboard and pointing device connected to one Mac to control multiple Macs and iPads. Despite the feature appearing in macOS 12.3 and iPadOS 15.4, Apple labels it as a beta, suggesting that users may still encounter hiccups.

Even for a beta, the experience is nearly seamless. Once you've set up Universal Control in System Preferences > Displays, you can move your pointer from one Mac to another Mac or an iPad and back, just as though they were external monitors making

up an extended Desktop. Keyboard focus—which device receives typed keystrokes—follows the pointer, so once you move the pointer to another device and click an app, that device behaves just as though you're using it directly. With an iPad, it acts though you have connected a trackpad and hardware keyboard (see "[The iPad Gets Full Trackpad and Mouse Support](#)," 28 March 2020). Even better, you can drag files and other items between devices.

It's important to distinguish Universal Control from Sidecar, Apple's technology for turning an iPad into a secondary display for the Mac (see "[Catalina's Sidecar Turns an iPad into a Second Mac Monitor](#)," 21 October 2019). Sidecar still exists and, in fact, shares a menu with Universal Control

in the Displays preference pane. Similarly, with Macs, you need to differentiate between viewing a screen with AirPlay and controlling it using Universal Control. More on that shortly.

Although we don't know Universal Control's provenance, it's far from a new idea, at least with regard to controlling one Mac from another. Fifteen years ago, Adam Engst used a utility called Teleport that provided exactly these features (see "[Tools We Use: Teleport](#)," 27 August 2007). Even more interestingly, Teleport developer Julien Robert worked for Apple then and reportedly continues to do so. A little birdie tells us that Teleport has even continued to receive private updates inside Apple. It also turns out that Teleport was open-sourced some years ago. [John Britton has been maintaining it](#), providing a Mac-only option for those not running macOS 12.3 everywhere.

Universal Control Requirements

Before getting started, make sure your [devices support Universal Control](#). Hardware support goes back some years, although Universal Control does *not* support all Macs that can run Monterey or iPads compatible with iPadOS 15. Also, make sure that:

- All devices are signed in to the same iCloud account
- Bluetooth and Wi-Fi are enabled on all devices
- Handoff is enabled in System Preferences > General on the Mac and in Settings > General > AirPlay & Handoff on the iPad
- Your Apple ID is set up for two-factor authentication
- The devices are within 30 feet (10 meters) of each other
- Neither the Mac nor iPad is sharing its Internet connection

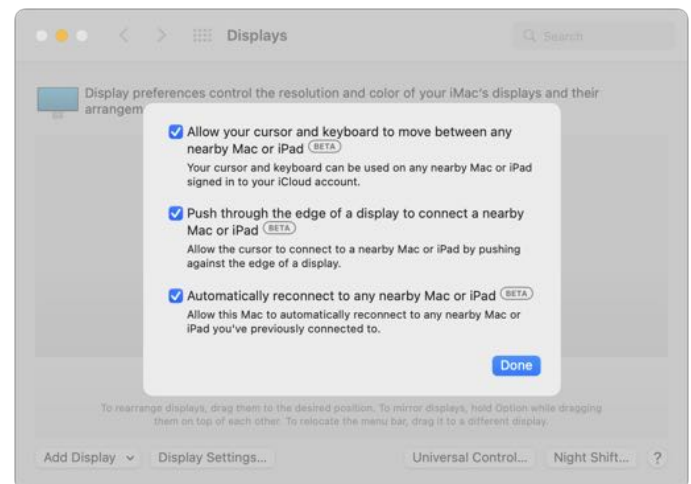


<https://youtu.be/9tRzhE-wyNg>

With Universal Control, you can connect and control up to three additional devices from your Mac at one time. Mix and match however you would like, whether that means controlling three other Macs, three iPads, two Macs and an iPad, or two iPads and a Mac. We suspect that's more than enough since it will get difficult to arrange even that many devices in a usable fashion. Remember, Universal Control must be initiated from a Mac, so you need a Mac in the mix somewhere.

Setting Up Universal Control

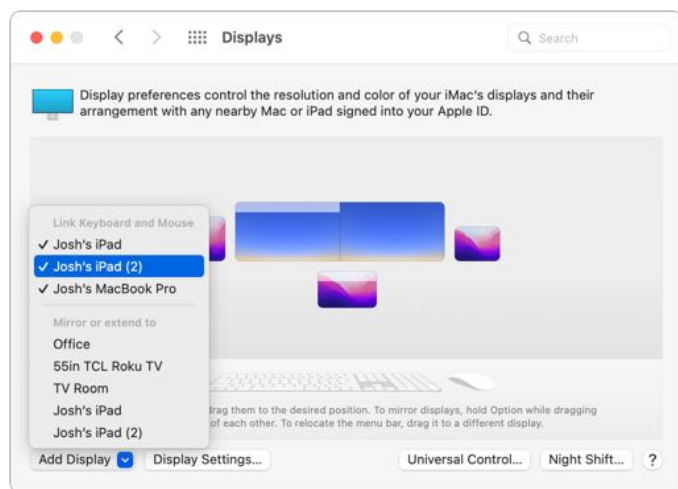
Universal Control is simple to set up. On all your Macs, open System Preferences > Displays and click Universal Control. Select all three of the checkboxes. The first one—"Allow your cursor and keyboard to move between any nearby Mac or iPad"—is Universal Control's primary switch.



On an iPad, go to Settings > General > AirPlay & Handoff and make sure Cursor and Keyboard is enabled.

That may be all you need to do, thanks to the “Push through the edge of a display to connect to a nearby Mac or iPad” checkbox. When selected, that lets you connect by moving the pointer from your Mac to the other device, just as you’d do with an external display. Available Macs and iPads should appear in System Preferences > Displays.

In the Displays preference pane, you can—and should—drag the display thumbnails around to make them better match their real-world relative positions on your desk. Otherwise, it’s difficult to move the pointer between devices fluidly. Unlike secondary displays, which abut their Mac’s primary display, thumbnails representing Universal Control devices are separated slightly, as you can see below.

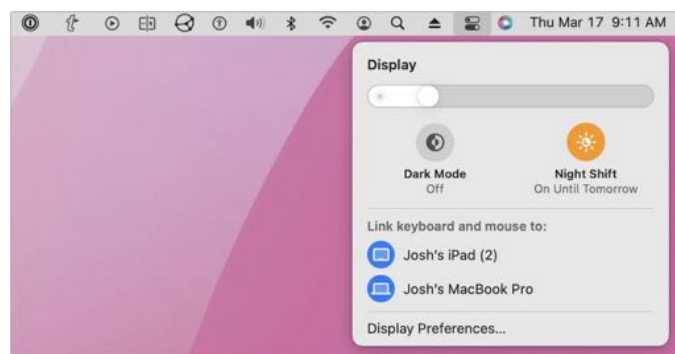


If the desired Mac or iPad doesn’t automatically appear in the Displays preference pane, from the Add Display pop-up menu, select the device you want to control under “Link Keyboard and Mouse.” As long as you’ve selected “Automatically reconnect to any nearby Mac or iPad,” you shouldn’t have to repeat this step.

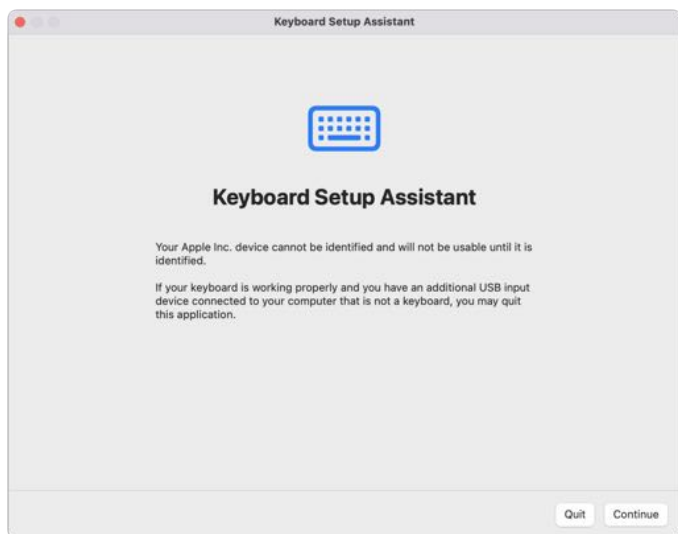
Note the “Mirror or Extend to” section of the Add Display pop-up menu. That’s how Apple provides access to Sidecar, which lets you use an iPad as a secondary display for the Mac, mirroring or extending its Desktop. You’ll also see Macs running Monterey (which can act as an AirPlay receiver) and Apple TVs in this menu. You can select an iPad or Mac in only one of the two sections at a time. In other words, you can’t control an iPad or Mac via

Universal Control while simultaneously using it as a secondary Mac display. That makes sense because Universal Control lets you drive the device’s native interface, whereas Sidecar / AirPlay hides the native interface behind the Mac’s secondary display. There’s no harm in switching back and forth between Universal Control and Sidecar / AirPlay.

If the automatic connection doesn’t work, you can also connect to another Mac or iPad through the Mac’s Control Center by clicking Display and selecting a device under “Link keyboard and mouse to.” The device icons show as gray when they’re merely available and change to blue when you select them.



One oddity: The first time I connected to a new device, the Keyboard Setup Assistant appeared on the initiating Mac, presumably because of a mismatch between the new keyboard and the device’s native one. You can click Continue to identify the keyboard or even just click Quit—I saw no issues either way. The Keyboard Setup Assistant never appeared for Adam Engst in his testing, so it must be related to something associated with macOS settings or state.



Given that Universal Control remains in beta, it shouldn't be surprising that there are rough edges. At one point, it wouldn't let me add a second iPad—telling me I had already reached the limit with two devices—until I put the also-connected MacBook Pro to sleep. After I connected the second iPad, I woke up the MacBook Pro, and all three devices worked fine.

Using Universal Control

If you've ever used multiple monitors on a Mac, Universal Control will seem instantly familiar. Depending on how you have your screens arranged in the Displays preference pane, when you move your pointer off-screen in the direction of another device, the pointer will jump to that device. It works that way both on the Mac and iPad. Once the pointer is on another device's screen, you can use that device just as though you were controlling it directly.

As you would expect, moving from a Mac to an iPad is a little jarring since the pointer changes from an arrow to a little circle and switches to the iPadOS pointing-device paradigm, which is a hybrid between a traditional pointer and a touchscreen. Most notably, the pointer is attracted to Home screen icons and many other controls, which transform it into a selection highlight. Regardless, in basic usage, Universal Control just works.

Universal Control provides two additional capabilities that make it easy to move data from one device to another. First, you can copy data on one device with Command-C, move the pointer to another device, and paste into an app on the second device with Command-V. The fact that copy-and-paste is foundational technology makes it no less welcome. We don't know exactly how Universal Control implements clipboard sharing, but it seems faster and more reliable than Apple's [Universal Clipboard](#) technology, which also shares clipboards between your devices.

Second, you can drag and drop items between two Macs or even between a Mac and an iPad. The obvious use is moving files between Macs, but Apple suggests you could also drag a sketch from the iPad to your Mac or move a photo from your Mac into a Messages conversation on your iPad. The Messages example doesn't make much sense because you could more easily drag into Messages on your Mac.

Since each Mac in a Universal Control set is running independently—additional Macs are *not* secondary displays—you can't drag a window from one Mac to another, as you would from a Mac to its external monitor.

Universal Control Quirks

Although Universal Control works extremely well, some inevitable oddities crop up in actual usage.

- **All devices are (nearly) equal participants:** Once you've turned it on, Universal Control has no concept of primary and secondary devices. If you have an iMac and a MacBook Pro sitting next to each other, you can use the iMac's keyboard and mouse to control the MacBook Pro, but you can also use the MacBook Pro's keyboard and trackpad to control the iMac. Similarly, you can use a connected iPad's trackpad and keyboard to control Macs.
- **Losing the pointer:** With multiple screens in play, it can be easy to lose your pointer. On a Mac, you can “shake” the pointer to make it grow in size and become easier to spot. However, that won't work if the pointer is on the iPad. Here's

a little trick to solve that problem: if you move your pointer using another Mac, it will appear in the center of that Mac's screen. Let's say you're using an iMac and MacBook Pro together, and you lose track of the pointer but need to click something on the MacBook Pro. Just touch your MacBook Pro's trackpad, and the pointer appears in the center of its screen, ready to go wherever you want.

- **Keyboard shortcut conflicts:** One of the small confusions of controlling an iPad with your Mac's keyboard is that the same keyboard shortcuts may have different results on each platform. For example, typing Command-H while using the iPad simulates pressing the Home button. However, Command-H hides windows on the Mac. Unless you're certain which device is receiving keystrokes, you can end up with unpredictable behavior.
- **Click for keyboard focus:** Making the previous problem worse is the fact that simply moving the pointer from one device to another isn't enough to transfer keyboard focus. You must also click somewhere on the destination device. If you forget to click, you can end up in a situation like this: Start typing in a window on your Mac, move your pointer to an iPad showing an active note in Notes, and type a few more characters. You might think your keystrokes would go to the iPad, but you'd be wrong—without that additional click in an app on the destination device, you'd still be typing into the window on the Mac.
- **Click for Mac pointer focus:** The focus issue also affects some mouse clicks between Macs—your first click will make the clicked app active, and the second one will activate the button or link. That's not always the case on Macs, and it never seemed to crop up in our iPad testing. We suspect those who use Universal Control will develop the habit of clicking as soon as they move the pointer to a new device.
- **Keyboard-centric sleep while using an iPad:** Say you have your Mac set to turn its display off

after 1 minute. You then use Universal Control to work on your iPad. As long as you use the keyboard, there's no problem. But if you're just reading, using your trackpad or scroll wheel to scroll, the Mac will turn its display off after 1 minute and break the Universal Control connection. Press a key, and the Mac wakes up to its login screen. This seems to happen only when using an iPad—additional Macs keep their screens on while being controlled despite their screen sleep settings. If you plan to use Universal Control regularly, consider increasing the "Turn display off after" time in System Preferences > Energy Saver / Battery on Macs from which you'll control iPads.

- **Not all drags work:** I was able to drag a photo from the Photos app on the Mac to the Files app on an iPad, but trying to drag a photo from Files on the iPad to Signal on the Mac failed. I suspect that individual developers will have to adjust their apps to accept items dragged over from another device. Copy and paste may work in such situations, or you could always fall back on AirDrop or iCloud Drive.

Again, we are talking about a beta here. We saw several instances where a remote Mac or iPad stopped accepting clicks or fell out of the Universal Control set entirely. In the case of iPads, putting it to sleep and waking it back up usually fixed the problem. Other times we had to select the recalcitrant device from the Add Displays pop-up menu in the Displays preference pane. We expect most such issues to disappear as Apple updates macOS and iPadOS.

Universal Control: Refilling a Hole in the Universe

Universal Control is a tremendously cool feature, even if it merely brings Teleport back to the masses and extends it to iPadOS. The simple fact of the matter is that Teleport hasn't been a well-known solution for many years, forcing those who wanted to use the same keyboard and pointing device with

multiple Macs to use a hardware switch that could cost \$50 to \$500, depending on its capabilities.

With Universal Control, Apple is adding a core feature to its ecosystem, one that further integrates different devices. Apple doesn't want you to replace your Mac with an iPad; it wants you to buy an iPad and a Mac. And now you can use them together more easily than ever before. For many, just being able to flip back and forth between their Macs and iPads will be a huge win—that's undoubtedly the prime use case.

Some people may see Universal Control as a way to increase screen real estate by using multiple Macs simultaneously. It's probably not worth buying new Macs for that purpose, but it might be a great way to keep an older MacBook Pro useful after purchasing a new Mac Studio, for instance. The downside is, of course, that you have to keep both

Macs up to date and figure out the best way to sync data between them.

Finally, if you're more iPad-focused than we are, you could also dedicate an iPad on your desk to a single app that either doesn't exist on the Mac or doesn't work as well. Universal Control might also be a fluid way to move iPad-only content to the Mac, such as drawings created with an Apple Pencil.

A Note Just In Case...

Universal Control does not work with iPhones. See the System Requirements in the Apple Support article.

Apple Support Universal Control: Use a single keyboard and mouse between Mac and iPad

Use the keyboard, mouse, or trackpad of your Mac to control up to two other nearby Mac or iPad devices, and work seamlessly between them. 🖱️

