February 2024
Vol. XLIII, No 2

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral February 20th 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

- iPhone Protection
- macOS 14 Sonoma
- Clean My Mac

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 Adam Engst

Apple’s End-of-Year OS Updates Add Promised Features, Security Updates

It wasn’t surprising when Software Update suddenly started offering iOS 17.2, iPadOS 17.2, macOS 14.2 Sonoma, watchOS 10.2, tvOS 17.2, and HomePod Software 17.2. All but the last come with new and enhanced features that Apple promised but didn’t include in the initial releases. (Apple regularly schedules operating system updates in early to mid-December so its engineers can enjoy the holidays and users can explore the new features during the downtime.)

Given how feature-rich these releases are, I encourage waiting a week to ensure they don’t introduce unexpected problems. Then install the updates at a point when, if something goes wrong, you won’t be forced to troubleshoot tech issues during family holiday time. That’s always awkward.

Apple also released security fixes for older operating systems: iOS 16.7.3 and iPadOS 16.7.3, macOS 13.6.3 Ventura, and macOS 12.7.2 Monterey. Note that the iOS and iPadOS updates address the WebKit vulnerabilities Apple previously said had been exploited against versions of iOS older than iOS 16.7.1, which I incorrectly interpreted as suggesting iOS 16.7.2 wasn’t vulnerable (see “WebKit Zero-Day Vulnerabilities Prompt iOS 17.1.2, iPadOS 17.1.2, macOS 14.1.2, and Safari 17.1.2,” 1 December 2023). If you’re stuck on iOS 16, I recommend updating sooner rather than later.

iOS 17.2 and iPadOS 17.2

The marquee feature of iOS 17.2 is the addition of Apple’s Journal app, which even warranted an Apple Newsroom article. Although developers have offered many journaling apps on the iPhone since the App Store opened, Apple seems to be claiming it was worth releasing its own because it’s so important to “practice gratitude and improve wellbeing.” Journal isn’t just a case of Apple “Sherlocking” the competition, though. One of Journal’s main features is that it leverages “on-device machine learning to provide private, personalized suggestions to inspire journal entries,” and Apple has opened that API up to third-party journaling apps so they can also suggest moments to write about. I tend to agree with Dan Moren, who suggests at Six Colors that there are people who like journaling (and are unlikely to switch to Journal) and those who don’t (and are unlikely to start).

Other notable improvements to iOS 17.2 or both iOS 17.2 and iPadOS 17.2 include:

- The Action button on the iPhone 15 Pro and iPhone 15 Pro Max gains a Translate option for those needing frequent translations.
- The Camera app on the iPhone 15 Pro and iPhone 15 Pro Max offers faster focusing speed when using the Telephoto camera to capture small, faraway objects. It also lets users of those iPhones capture spatial video for three-dimensional viewing on the Apple Vision Pro headset, which is due next year. Spatial video won’t look different when viewed elsewhere.
- Messages gains a catch-up arrow that lets you jump to the first unread message in a conversation, gives you the ability to add a sticker directly to a message bubble, allows you to adjust the body shape of your Memoji, and introduces Contact Key Verification (see “Upcoming Contact Key Verification Feature Promises Secure Identity Verification for iMessage,” 8 November 2023).
- The Weather app provides precipitation amount forecasts for the next 10 days, adds a handful of new widgets, provides a wind map snapshot to assess wind patterns, and gives

you an interactive moon calendar for visualizing moon phases over the next month.

- Siri gains support for accessing and logging Health app data using your voice—it's on-device only to protect privacy.
- AirDrop extends the NameDrop approach of holding two iPhones close together to share boarding passes, movie tickets, and what Apple loosely describes as "other eligible passes."
- The new Favorite Songs playlist in Apple Music collects the songs you've marked as favorites. If it doesn't appear for you, as it didn't for me, mark a new song as a favorite, after which it should show up with all your previously favorited songs.
- You can disable Apple Music's Use Listening History in a Focus to prevent music you listen to while in that Focus from appearing in Recently Played or influencing recommendations. Workout or studying music might differ from what you usually want to listen to.
- There's supposedly a new Digital Clock widget for use on the Home Screen and in StandBy on the iPhone, and on the Home Screen and Lock Screen for the iPad. I'm unsure what to look for here—nothing jumps out at me.
- Enhanced AutoFill identifies forms in PDFs and helps you populate them with information such as names and addresses from Contacts.
- A Sensitive Content Warning for stickers in Messages prevents you from unexpectedly being shown a sticker containing nudity. How long did it take teenagers to find that loophole?
- iPhone 13 and iPhone 14 models gain support for Qi2 wireless chargers that are starting to hit the market. The iPhone 15 lineup is already compatible.
- There are new keyboard layouts for eight Sámi languages used by the Sámi-speaking peoples in northern parts of Norway, Sweden, and Finland, and of the Kola Peninsula in Russia. (Thank you, Wikipedia.)

The only bug fix that Apple admits to resolves problems with wireless charging in certain vehicles, but iOS 17.2 also addresses 10 security vulnerabilities, none of which are being actively exploited in the wild.

macOS 14.2 Sonoma

Most of the features in iOS and iPadOS appear in macOS as well. So macOS 14.2 gains PDF Enhanced AutoFill, Messages improvements, Weather enhancements, Favorite Songs playlist, Use Listening History carve-out, and keyboard layouts for seven additional Sámi languages.

There are just two Mac-specific improvements:

- The Clock app now supports multiple timers, timer presets, and recent timers, bringing the Mac into parity with other devices.
- Shazam Music Recognition now lets you identify songs playing around you even when you're wearing AirPods.

Apple's release notes don't mention any bug fixes, but there are also fixes for 21 security vulnerabilities, none of which are being actively exploited in the wild.

watchOS 10.2

As with iOS 17.2 and iPadOS 17.2, watchOS 10.2 lets you access and log Health app data using Siri—instrumental on the Apple Watch—but only for two models: this year's Apple Watch Series 9 and Apple Watch Ultra 2.

The other changes refine several of the new interface approaches that appeared in the initial release of watchOS 10:

- Apple added an option to Settings that returns the ability to swipe to change watch faces, the absence of which irked many users. I couldn't find it, but *Take Control of Apple Watch* author Jeff Carlson revealed that Apple hid it in Settings > Clock on the Apple Watch itself;

there's no corresponding option in the iPhone's Watch app.

- Another Settings option—in Settings > Workout—lets you control whether or not you need to confirm when a workout ends.
- Now Playing appears automatically whenever an Apple Watch is near a second-generation HomePod or a HomePod mini playing media from Music or Podcasts; it requires an Apple Watch Series 6 or later.
- In most Apple Fitness+ workouts, you can now prioritize the volume of either the music or the trainers' voices.

The only bug fix listed resolves a problem that prevented watch faces added in the iPhone's Watch app from appearing on the Apple Watch. watchOS 10.2 also fixes 8 security vulnerabilities, two of which are the WebKit vulnerabilities we covered in "WebKit Zero-Day Vulnerabilities Prompt iOS 17.1.2, iPadOS 17.1.2, macOS 14.1.2, and Safari 17.1.2" (1 December 2023).

tvOS 17.2

Surprisingly, tvOS 17.2 received quite a bit of attention from Apple. Most notably, the company redesigned the Apple TV app, adding a sidebar for faster navigation. Within the sidebar, Watch Now has been renamed to Home, and within Home, the Channels & Apps section lets users focus on subscribed channels and connected apps. I have long found the TV app's interface to be a mess that tries to do more than is feasible in such a limited space; we'll see if this redesign makes a difference or just moves deck chairs around.

Also, the iTunes TV and iTunes Movies apps are now just shells of their former selves that redirect to the TV app, where you can buy or rent shows and movies. Finally, although Apple doesn't mention it in any of the other release notes, these changes are also reflected in the TV apps in iOS 17.2, iPadOS 17.2, and macOS 14.2.

The other significant change in tvOS 17.2 comes with the FaceTime app, which Apple introduced in tvOS 17. That initial version lacked a few key FaceTime features: you can now answer calls directly on the Apple TV, participate in FaceTime Audio calls, and move calls from your Apple TV to your iPhone or iPad. (FaceTime on the Apple TV requires at least a second-generation Apple TV 4K.)

Other improvements include:

- SharePlay now supports Dolby Atmos and Dolby Digital surround sound formats.
- Apple Fitness+ lets you prioritize music or trainer voices, just as in watchOS 10.2.
- You can press the Siri button on the remote to start an onscreen search anywhere inside supported apps like TV and Music.
- Siri now includes language support for Arabic in Saudi Arabia and United Arab Emirates, Malay in Malaysia, and Turkish in Türkiye.

Continuing the trend from the other updates, Apple's release notes mention no bug fixes, but tvOS 17.2 addresses 7 security vulnerabilities, including the previously fixed WebKit bugs.

HomePod Software 17.2

Nothing but "performance and stability improvements" to see here, folks.

Move along.

By Adam Engst

Apple to Introduce Stolen Device Protection in the Upcoming iOS 17.3

Remember the stellar reporting by the Wall Street Journal's Joanna Stern and Nicole Nguyen about how thieves could shoulder-surf someone entering their iPhone passcode, snatch the iPhone, and then use the passcode to reset the victim's Apple ID password? We covered it in "How a Thief with Your iPhone Passcode Can Ruin Your Digital Life" (26 February 2023) and "How a Passcode Thief Can Lock You Out of Your iCloud Account, Possibly Permanently" (20 April 2023). The much-shared Screen Time passcode is easily bypassed, so the only practical protections were:

- Pay attention to your iPhone's physical security in public.
- Always use Face ID or Touch ID in public.
- If you must use your passcode in public, conceal it from anyone nearby.
- Never share your passcode beyond highly trusted family members.

Even then, the journalists revealed incidents of drugging and assault for which those four principles wouldn't have helped at all.

Stern and Nguyen are now reporting that Apple has included a new Stolen Device Protection feature in the current beta release of iOS 17.3, which I expect Apple to release to the public in January or February 2024. Stolen Device Protection tries to minimize the potential of passcode theft by relying more heavily on biometric authentication and familiar locations, like your home and work.

With the feature enabled, when you want to change your Apple ID password or add a recovery key (which thieves used to lock victims out of their iCloud accounts), there are no new requirements as long as you're at what your iPhone believes to be a familiar location (like home or work). However, when you're anywhere else, your iPhone will require two Face ID or Touch ID scans an hour apart before completing those actions. Requiring just one biometric authentication blocks the snatch-and-grab approach because the passcode won't be sufficient on its own to do anything. Requiring the second scan an hour later ensures that even a forced scan during a mugging or drugging won't be sufficient unless you've been held hostage for that time.

One concern is that viewing Settings > Privacy & Security > Location Services > System Services > Significant Locations must also require biometric authentication, or else the thief could go to one of those locations to complete the takeover. In iOS 17.2, viewing that screen requires Face ID or Touch ID, but failures can be overridden with the passcode.

Additional features that require two biometric scans with an hour gap when initiated from an unfamiliar location include changing a trusted phone number or contact, adding another face to Face ID or fingerprint to Touch ID, turning off Face ID or Touch ID, disabling Find My, and turning off Stolen Device Protection.

Another significant impact of passcode theft was that the thief could access the victim's passwords in iCloud Keychain. If you turn on Stolen Device Protection, that will no longer be possible: accessing passwords will require Face ID or Touch ID authentication. Other features that will require biometric authentication (but not the hour wait) include applying for a new Apple Card, erasing all content and settings, turning off Lost Mode, sending Apple Cash to a bank account, using the iPhone to set up a new device (which copies all the data), and using payment methods saved in Safari. It's the first time Apple has required Face ID or

Touch ID instead of a device passcode to prove one's identity or intent.

Apple won't turn Stolen Device Mode on for you, but iOS 17.3 will alert users to the feature when they update. That seems reasonable for the first release, and I plan to turn it on. I wouldn't be surprised if a future iOS version were to push it strongly during setup as Apple has increasingly done with other security features, including two-factor authentication for Apple ID accounts (required in nearly all cases now) and Find My (heavily promoted during upgrades if not already enabled).

Why would someone not want to enable Stolen Device Protection? Some people experience poor results with Touch ID—less so with Face ID—so leaving it off needs to be an option for them. I can also imagine it possibly introducing friction while traveling, but that may be a reasonable tradeoff for the increased chance of being robbed while on vacation.

People who avoid biometric authentication because they think biometrics are less secure than passcodes can continue to be wrong. Ironically, they may end up at less risk if the herd immunity of wide adoption of Stolen Device Protection causes thieves to give up on passcode theft as not worth the minimal reward. (It seems like Authentication Lock and Find My had some deterrent effect when introduced years ago.)

I look forward to seeing reports on the impact of Stolen Device Protection on users. Those who spend most of their time in familiar locations probably won't even notice its additional requirements. The people for whom Stolen Device Protection would be the biggest pain are those who forget their Apple ID password and want to reset it immediately via their device without having to go through a process and an hour wait—although I would wager most people in that scenario are at home or work, thus sidestepping the wait.

Finally, just because you turn on Stolen Device Protection doesn't prevent a thief from stealing your passcode and your iPhone, and accessing any apps that don't require an additional PIN or biometric authentication. Make sure to enable such layered authentication in any app that manages money or sensitive information.

And, as I said initially, just don't use your passcode in public.

By Glenn Fleishman

How To Avoid AI Voice Impersonation and Similar Scams

AI voice impersonation puts a new twist on an old scam, and you and your family need to be prepared. Forewarned is forearmed when criminals can take snippets of online audio and use increasingly widely available tools to make a sufficiently convincing AI voice, bolstered by claims to be on a poor phone connection.

I encourage you to have conversations among your family, at least—but maybe also within your company or social groups—so everyone is aware that these kinds of scams are taking place. The best defense relies on a shared secret password or other information only you and the purported caller would know.

How the Scam Works

The kind of fraud related to AI voice impersonation is typically called the "grandparent scam." It works like this: The phone rings in a grandparent's home, usually early in the morning or late at night. They answer, and it's one of their grandchildren saying they have been in an accident, arrested, or robbed. They need money—fast. The connection is often poor, and the grandchild is in distress.

"Is this really Paolo? It doesn't sound quite like you."

"Grandma, it's me. I'm on that trip to Mexico I told you about, and thieves stole my wallet and phone! Can you wire me some money so I can get a new phone?"

The grandparent leaps to help by running to a Walmart or Western Union—or even withdrawing cash from a bank and handing it off to a "courier" who arrives at their home. And their money is off to a scammer.

The FBI says this particular scam first reared its head in 2008, likely because of the confluence of inexpensive calls from anywhere, the ease of transferring money worldwide instantly, and social media making it easier for fraudsters to discover facts about people that let them make plausible assertions.

Of course, this scam doesn't always involve grandparents, and I don't mean to imply that older people are more easily fooled. Scammers also target children, parents, distant relatives, friends, neighbors, and co-workers. Sometimes the caller alleges to be a police officer, a doctor, or, ironically, an FBI agent.

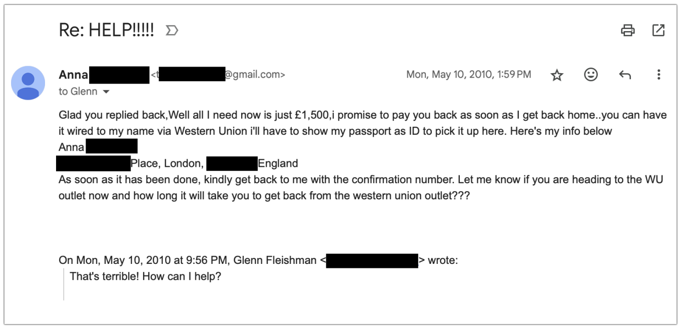
The key element of the scam is that a close family member, friend, or colleague is in dire need. The purported urgency and potential threat against the caller's freedom or ability to return home override the normal critical thinking most people would bring to bear. The scammers also often call in the middle of the night when we're less likely to be alert, or attempt to take advantage of cognitive declines or hearing problems in older family members.

The AI voice impersonation aspect adds a "future shock" element: none of us are prepared for a call from a thoroughly convincing version of someone we know well. It's already happening. The FTC highlighted it in a post on March 2023. And you can find news accounts around the country, meaning it's just a slice of the whole scam ham: the Washington Post on a Canadian fraud, March 2023; Good Morning America, June 2023; New Mexico, September 2023; and San Diego, November 2023; just for instance. Posts on forums abound, too, like Reddit.

Services arose last year that can produce a credible voice impression from fairly small amounts of audio, notably ElevenLabs. The AI voice is eerily accurate when seeded with a few minutes of audio. It doesn't cost much to generate a voice clone, and many services have few or no safeguards to prevent misuse, a variety of which happened almost immediately. The FTC is soliciting proposals on how to identify and deter voice cloning fraud.

It's unclear how the scammers acquired a recording of the person's voice in some cases. Obviously, if someone is a podcaster or appears in YouTube or TikTok videos, those are likely sources. But it's also plausible that a generic voice of the right age and accent could fool people. There's an outlier that's occurred, too: a caller, who had to be an AI, tried to scam a grandmother in Montreal in part by dropping in Italian nicknames, like calling her *Nonna*. That's uncanny and would have required a high degree of research for a relatively small financial gain.

These scams can also come in by email, though they are often far less convincing due to less of a feeling of urgency, as well as issues with diction, spelling, and other written factors. I received this email in 2010 from my "friend" Anna. The real Anna was someone I knew and liked but wasn't close enough to for her to ask me to borrow a pile of money, and she was well-spoken and careful with words in my interactions with her. The first email was brief; I replied and got what you see below. It's not convincing—but that was before we had generative AI penning such letters.



Re: HELP!!!!!

Anna [redacted] <t[redacted]@gmail.com> Mon, May 10, 2010, 1:59 PM

to Glenn

Glad you replied back,Well all I need now is just £1,500,i promise to pay you back as soon as I get back home..you can have it wired to my name via Western Union i'll have to show my passport as ID to pick it up here. Here's my info below
Anna [redacted]
[redacted] Place, London, [redacted] England
As soon as it has been done, kindly get back to me with the confirmation number. Let me know if you are heading to the WU outlet now and how long it will take you to get back from the western union outlet???

On Mon, May 10, 2010 at 9:56 PM, Glenn Fleishman <[redacted]> wrote:

> That's terrible! How can I help?

The Robots Are Coming for Your Money

You can beat most of these scams with a shared password among family, friends, or co-workers. As with most aspects of verification, the process requires an *out-of-band* channel for information. Essentially, you want to provide a secret or details over a communication method that isn't the same one you're securing with that information. (We write about the out-of-band issue so much at TidBITS, we should form a musical group called "Out of Band")

Your group should set up a password for situations where you need to confirm identities over the phone. Let's say it's "raspberry beret." If you get a call from a loved one in trouble, you can say, "Look, there are scams, and we talked about this—what's the password?" The password should be something familiar that's easily remembered but not associated with you online. A family joke can be good. You don't have to be strict about them getting it perfect—you're not verifying their nuclear launch code authority.

If the caller can't remember the password, dig deeper and ask for personal facts—they should be readily available to a person you know well. "Do you remember what Uncle Don told you?" "No, I don't remember what he said." "You don't have an Uncle Don." (As a result of researching this article, my family now has a password.)

You can also identify and defeat these scams through simple means:

- While stalling the caller (pretend to be sleepy or confused), surreptitiously text the person at their known phone number to confirm their situation.
- Say you'll call them back, then call the person's known phone number. A criminal will likely claim that their phone was stolen or not working. In many of the stories linked above, when the scam failed, it was because the victim placed a call or sent a text.
- Try to get them to switch to a video call "like you always do." So far, AI isn't good enough to provide live video impersonation of an arbitrary person.
- Call or text a relative or other person in common who might be more informed about the alleged caller's location if they can't be reached immediately.
- Call a police station where the person claims to be calling from.

I also hope all TidBITS readers know this, but police departments and lawyers never ask for funds to be wired through Western Union, Walmart or Amazon gift cards, Bitcoin, or the like; they don't demand the money be sent immediately; they don't make threats; and they don't tell you not to call anyone to confirm the facts. While behavior like that should cause even the most trusting person to take notice, we'll rarely be in these situations in our lives, so we can be taken unaware. It's essential to consider the possibilities ahead of time to establish the pathways you'll need to defeat scams under pressure.

I mentioned earlier that email can be much less convincing, using the example of my friend-of-a-friend's hijacked email account and message. So I asked ChatGPT to compose an email to my grandmother telling her I was robbed in Mexico and my cameras were stolen. The first try was stilted, so I told it to use simpler, less formal language. On the second try, it came up with what could be a convincing message with no red flags:

Subject: N*eed Help Grandma! Got Robbed in Mexico* 😟

Hey Grandma,

Hope you're doing okay! So, guess what? I'm in Mexico right now, but something crazy happened. I got robbed! Yep, they took my cameras and some other stuff. But don't worry, I'm totally fine, just a bit shaken up.

I really need your help with this. Can we talk about it soon?

Miss you and can't wait to see you!

[Your Name]

No, ChatGPT, no! Generative AI assistance can easily eliminate the usual unconvincing use of language, idiom, and tone that characterize most "grandparent scam" attempts. Imagine an email interchange or live chat with someone who sounds like someone you know and love, trust, or work with, and who can answer a lot of basic questions. That's why you must be ready with a shared password, backchannel confirmation, or video chat.