

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral March 19th 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

- Exploring iOS 17
- FaceTime remote control screen sharing



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

KeystoneKeystone MacCentral March Meeting	1
Ventura and Monterey Users: Beware Unwanted Sonoma Upgrades By Adam Engst	3 - 4
Turn On Stolen Device Protection in iOS 17.3 By Adam Engst	5 - 7
How To Avoid AI Voice Impersonation and Similar Scams By Glenn Fleishman	7 - 9

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.

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

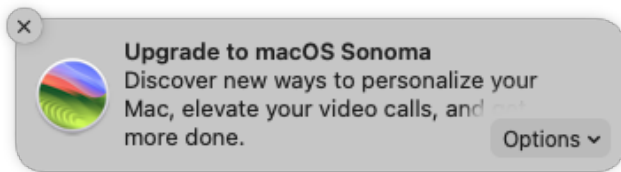
Tom Bank II



By Adam Engst

Ventura and Monterey Users: Beware Unwanted Sonoma Upgrades

Over the past week or so, reports have been accumulating from users who have dismissed a macOS notification encouraging an upgrade to macOS 14 Sonoma only to find themselves being upgraded anyway. [The first report on TidBITS Talk](#) came from Dave C., a developer and highly technical user who had intentionally been keeping his 2018 Mac mini on macOS 13 Ventura. When the notification appeared, he clicked the (X) button to dismiss it, but that was somehow interpreted as a positive consent to install.



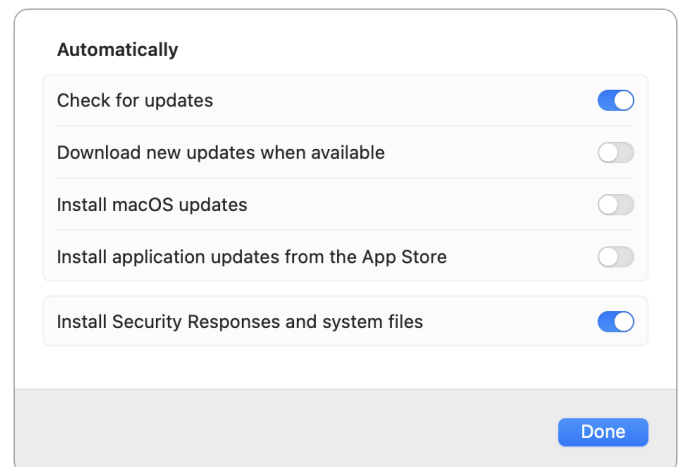
Unfortunately, starting with Ventura, Apple has moved from an upgrade process that involved downloading and launching an “Install macOS *versionName*” app to an update-like process that starts without giving the user an option to quit. [Howard Oakley suggests](#) the update approach dramatically reduces the amount of data that needs to be downloaded and shortens the installation time, but it lacks the flexibility of being able to stop the installer easily or point it at another drive.

Several other users on TidBITS Talk chimed in to say that they had also inadvertently triggered the Sonoma upgrade from that notification. Having read the warning post, when user [blm](#) dismissed the notification and saw the Sonoma upgrade start, they restarted their Mac immediately and were able to block the upgrade. [Jason Kerr](#) had a similar experience and was also able to shut down in time. [Will B.](#) triggered the update accidentally but didn’t realize until he was prompted to restart to install

it. He eventually prevented the upgrade from installing by turning the Mac off, rebooting into macOS Recovery, turning off [System Integrity Protection](#) (which protects certain parts of the system), deleting the downloaded upgrade files, and restarting.

[David Brostoff](#) waited a few minutes after dismissing the notification to shut down, but by then, it was too late, and he was upgraded to Sonoma. A few other users, including [anch-innk](#), [Ron LaPedis](#), and [Charles Reeves, Jr.](#) were upgraded to Sonoma even though they didn’t remember dismissing the notification. That’s almost more concerning.

In trying to figure out what was going on, TidBITS Talkers have confirmed that the problem affects both Intel-based and M-series Macs. Some were running macOS 13 Ventura and others macOS 12 Monterey. Being logged in as a standard user didn’t protect David C., whereas blm was logged in as an admin user. Nor did automatic update settings appear to be related—several people allowed macOS to “Check for updates” and “Install Security Responses and system files” but not “Download new updates when available” or “Install macOS updates.”



[Al Varnell](#) suggested that the notifications were triggered by a background update called `macOSInstallerNotification_RC` that was pushed to all Ventura users on 10 January 2024, which matches when these reports started. However, the mere presence of a notification shouldn't trigger updates when the user explicitly dismisses the notification.

[Will B.](#) spent 45 minutes talking to a courteous and sympathetic Apple Support Senior Advisor whose responses suggest that this situation is unintended on Apple's part. He encouraged those experiencing it to call Apple Support and submit reports through the Feedback Assistant app. In particular, he said that Engineering needs a report posted while the Mac is being threatened with the unwanted update so Feedback Assistant can grab all the relevant logs and provide a snapshot of the state of the machine.

There may be a few ways to forestall the upgrade:

- When faced with the Sonoma upgrade notification, choose Details or Info from the Options menu rather than clicking the (X) button.
- If you have clicked the (X) button, immediately open System Settings > General > Software Update (or System Preferences > Software Update) and look for a Cancel Update button.
- If that doesn't work, immediately restart the Mac to see if that interrupts the download and thus short-circuits the update process.
- If you are prompted to restart when you haven't initiated a restart, click Cancel. You'll probably be prompted again later, and if you restart manually, the upgrade will probably happen. Try following [Will B.'s approach](#) of booting to macOS Recovery, disabling SIP, and deleting the upgrade download.

If you're particularly concerned that you might inadvertently get Sonoma when you don't want it, it's possible turning off "Check for updates" in the

Automatically options shown above would help, but it's usually good to be alerted to new updates. P. Boersting also posted a set of steps to install a [profile that defers major upgrades](#). I haven't tested these, but they might be worth a try.

Stepping back from the nitty-gritty of this situation, I want to end with a few points:

- I don't believe Apple meant to force Sonoma upgrades on users. That's actively hostile behavior because there's no way of knowing why someone might be sticking with an older version of macOS or if it's a reasonable time to upgrade. It's unacceptable to trigger a major system update without explicit user permission, and I can't see Apple doing that deliberately. If nothing else, upgrading users like that doesn't benefit Apple in any material way.
- This is a nasty bug and is a distinct lapse on Apple's part. However, I think it's overstating the case to claim that it's indicative of a trend or a reason to stick with older versions of macOS. After all, the versions affected are Monterey and Ventura. Plus, because the bug doesn't affect everyone, it likely relies on specific circumstances that make it difficult to identify in testing.
- Although no one should be forced to upgrade by this bug, there's no reason to fear Sonoma. It has been out since September and has received several updates to fix bugs, add promised features, and block security vulnerabilities. I've been running it on my M1 MacBook Air since the beta with no particular issues and on my 27-inch iMac for about a month with no problems. If you buy a new Mac, it's what you'll get.

It's likely that Apple will quietly fix the bug behind the scenes and say nothing, so keep an eye on online discussions in TidBITS Talk and elsewhere to see when reports of these forced upgrades stop. 🙄

By Adam Engst

Turn On Stolen Device Protection in iOS 17.3

As promised, Apple built the new [Stolen Device Protection](#) technology into the just-released iOS 17.3. It offers optional protection against a particularly troubling form of attack brought to light by reporters Joanna Stern and Nicole Nguyen of the Wall Street Journal in a handful of articles and videos (see our “[iPhone Passcode Thefts](#)” series).

In short, a thief would discover the victim’s iPhone passcode by shoulder surfing, surreptitious filming, or social engineering, then grab the iPhone and run. In some cases, criminals drugged, threatened, or attacked people to extract the passcode. Soon after, the thief would use the passcode to change the victim’s Apple ID password, lock them out of their account, and use apps and data on the iPhone to steal money, order goods, and generally wreak havoc.

The attacks worked because Apple had made resetting an Apple ID password easy for those who could only remember their passcodes. Many people forget their Apple ID passwords, so Apple decided it was worth trading some security for allowing people to recover from a forgotten password easily. It also undoubtedly reduced Apple’s customer service overhead by providing a self-service option for resetting Apple ID passwords. Unfortunately, whenever there’s a loophole or backdoor, criminals will eventually find it.

Happily, Apple now lets us eliminate that security hole with Stolen Device Protection for iPhone. It’s not available for the iPad or the Mac. Apple hasn’t explained why, of course, but there are two possibilities for the iPad. Apple may be planning to add the feature to the iPad in a future update—the iPad often lags behind the iPhone—or the company may feel that iPad users are unlikely to be targeted similarly. (Many of the reported iPhone passcode thefts took place in bars where victims weren’t paying close attention and may have been impaired

by alcohol.) Macs seem even less likely to be targeted, given the additional difficulty of discovering a login password.

Stolen Device Protection Details

Here’s what happens when you turn on Stolen Device Protection. Everything works as before when you’re in a familiar location—home, work, or anywhere your iPhone has determined you use it frequently using the device-based [Significant Locations](#) system. You can change your Apple ID password, turn off Find My, access passwords in Keychain, and much more with no new requirements.

However, whenever you’re somewhere deemed unfamiliar, critical changes to your account or device require Face ID or Touch ID authentication, with no passcode alternative or fallback. The most important security actions also require a delay of an hour—shown with a countdown timer—before you perform a second biometric authentication. This delay reduces the chances of an attacker forcing you to authenticate with the threat of violence.

Apple says you must employ Face ID or Touch ID authentication in unfamiliar locations to:

- Use passwords or passkeys saved in Keychain
- Use payment methods saved in Safari (autofill)
- Turn off Lost Mode
- Erase all content and settings
- Apply for a new Apple Card
- View an Apple Card virtual card number
- Take certain Apple Cash and Savings actions in Wallet (for example, Apple Cash or Savings transfers)

- Use your iPhone to set up a new device (for example, Quick Start)

Notably, you can still use the iPhone passcode for in-person purchases made with Apple Pay, which remains a slight vulnerability. Apple likely felt that it would be too annoying to have a Face ID or Touch ID failure while attempting to pay for something at a store and not be able to fall back on the passcode.

You can also turn off Significant Locations with a passcode fallback after a biometric authentication failure, but all that does is eliminate familiar locations as a way of sidestepping biometrics. (Apple claims you must have Significant Locations enabled to use Stolen Device Protection, but that doesn't seem to be true, and deactivating it doesn't turn off the theft protection feature.)

Apple lays out which actions require the hour-long security delay and a second biometric authentication. These include when you want to:

- Change your Apple ID password (Apple notes this may prevent the location of your devices from appearing on iCloud.com for a while)
- Sign out of your Apple ID
- Update Apple ID account security settings (such as adding or removing a trusted device, Recovery Key, or Recovery Contact)
- Add or remove Face ID or Touch ID
- Change your iPhone passcode
- Reset All Settings
- Turn off Find My
- Turn off Stolen Device Protection

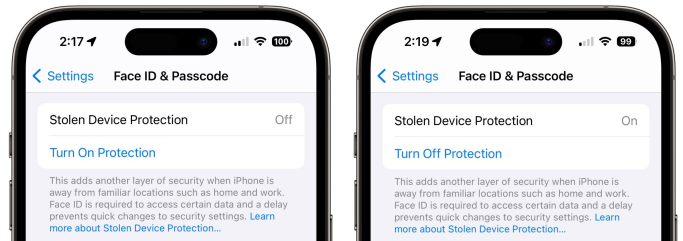
The security delay may end before the hour elapses if your iPhone detects that you've moved to a familiar location. In other words, you can short-circuit it by going home.

The fact that turning off Stolen Device Protection requires a security delay and biometric authentication means that you should be careful to turn it off before selling, giving away, or trading in

your iPhone. Once it's out of your physical control, it won't be possible for anyone else to reset it.

Turn on Stolen Device Protection

Turning Stolen Device Protection on is easy, and I recommend that everyone using Face ID or Touch ID do so. Go to Settings > Face ID / Touch ID & Passcode, enter your passcode, and tap Turn On Protection. (If it's enabled, tap Turn Off Protection to remove its additional safeguards.)



Stolen Device Protection does have a handful of requirements. Apple says you must:

- Be using two-factor authentication for your Apple ID (at this point, nearly everyone is)
- Have a passcode set up for your iPhone
- Turn on Face ID or Touch ID
- Enable Find My
- Turn on Significant Locations (Settings > Privacy & Security > Location Services > System Services > Significant Locations), although this doesn't seem to be required

Put bluntly, I can think of no good reason to avoid having all these required features enabled, anyway! With one exception, all increase your security with no privacy downside due to Apple's careful design and end-to-end encryption. In particular, anyone who believes Apple's biometric systems are less secure or private than a passcode is wrong and is putting themselves at risk.

The exception is Significant Locations because it displays the most recent significant location to anyone with the passcode. That makes possible—if not necessarily easy—the scenario of a thief learning your passcode, stealing your iPhone, and then going to the most recent significant location to

turn off Stolen Device Protection. You would likely have more time to lock the iPhone remotely, however.

Some individuals have trouble with biometric authentication, Touch ID more so than Face ID. The inability of every iPhone user to rely on biometric authentication is one big reason why Apple made Stolen Device Protection optional. If you're in that group, Stolen Device Protection would be problematic because it will require biometric authentication in unfamiliar locations. If you were on a trip, for instance, Stolen Device Protection and the inability to authenticate with Face ID or Touch

ID would prevent you from using passwords in Keychain.

I turned on Stolen Device Protection and triggered it by turning off Significant Locations and trying to turn off various security settings. Each time, I was met with a warning dialog and a security delay. Turning the iPhone off and back on merely stopped the security delay, forcing me to restart it. When it finally expires—an hour is a long time when you're testing!—iOS alerts you to that fact. You can then authenticate again and perform any of the previously restricted actions. 🗑️

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.

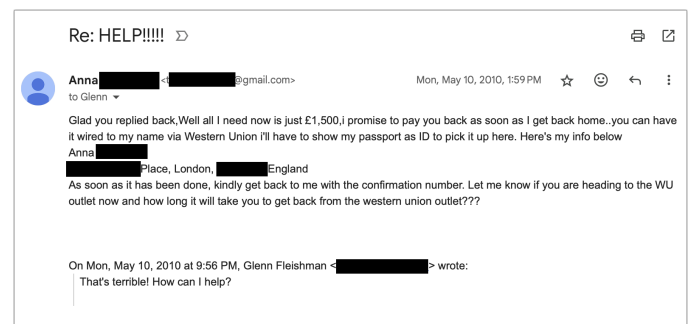
The AI voice impersonation aspect adds a "future shock" element: none of us are prepared for a call from a thoroughly convincing version of someone we know well. It's already happening. The FTC [highlighted it in a post](#) on March 2023. And you can find news accounts around the country, meaning it's 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.



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: Need 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. 🗣️