June 2022
Vol. XLI, No 06

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral June Program

June 21, 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

- Back up your Mac
- Best way to buy Microsoft office (or parts of it)
- USB-C & why you need it

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

By Adam Engst

Bad Apple #5: iCloud Drive Folder Sharing Risks Data Loss

I want to like iCloud Drive, I really do. As I noted in "Cloud Storage Forecast Unsettled, with Possible Storms" (4 February 2022), iCloud Drive is attractive for Apple users. It's reasonably priced, integrated into macOS and iOS, and unlikely to suffer from questionable privacy practices. On the downside, iCloud Drive has reliability problems that require toggling it off and back on periodically when it gets stuck—a Sync Now button and some decent logging to reveal what's happening would be welcome.

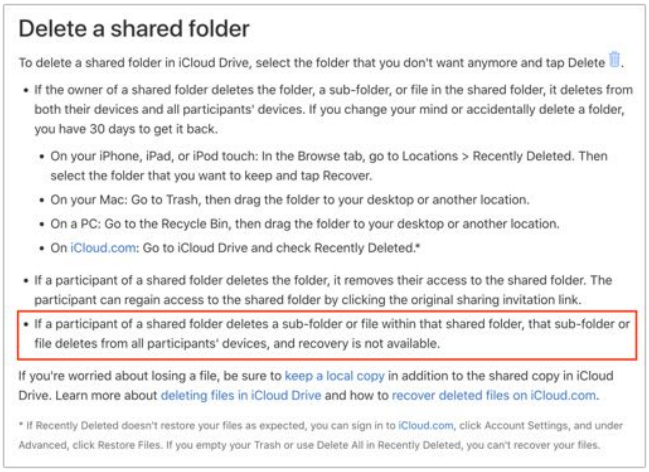
But this is the Bad Apple column, and Bad Apple articles don't complain about inadvertent bugs, nor do they address design decisions where reasonable people might disagree about the "right" way of doing something. Bad Apple articles call out something Apple has done intentionally but gotten utterly wrong.

Today's target is the discovery that when collaborators in an iCloud Drive shared folder delete files or folders, those items are destroyed instantaneously, not put in the Trash or added to iCloud Drive's Recently Deleted folder. They're just gone, with no option for recovery. If that's not bad enough—and it is—Apple has recently tweaked its already weak documentation in a way that further conceals this dangerous implementation. Bad Apple!

Quiet Warnings about Data Loss

Our story starts on 21 March 2022, when numerous Apple services, including iCloud Drive, became inaccessible for several hours. I was chatting with Paul Kafasis of Rogue Amoeba about whether the problem could be related to a Russian cyberattack or if it made more sense to invoke Hanlon's Razor: "Never attribute to malice that which is adequately explained by stupidity." The conversation segued into issues with iCloud Drive, including the desire for a Sync Now button, before Paul shared something he had discovered while researching a possible switch from Dropbox to iCloud Drive. In the main support article about iCloud Drive folder sharing, Apple made this statement:

If a participant of a shared folder deletes a sub-folder or file within that shared folder, that sub-folder or file deletes from all participants' devices, and recovery is not available.



Delete a shared folder

To delete a shared folder in iCloud Drive, select the folder that you don't want anymore and tap Delete.

- If the owner of a shared folder deletes the folder, a sub-folder, or file in the shared folder, it deletes from both their devices and all participants' devices. If you change your mind or accidentally delete a folder, you have 30 days to get it back.
  - On your iPhone, iPad, or iPod touch: In the Browse tab, go to Locations > Recently Deleted. Then select the folder that you want to keep and tap Recover.
  - On your Mac: Go to Trash, then drag the folder to your desktop or another location.
  - On a PC: Go to the Recycle Bin, then drag the folder to your desktop or another location.
  - On iCloud.com: Go to iCloud Drive and check Recently Deleted.*
- If a participant of a shared folder deletes the folder, it removes their access to the shared folder. The participant can regain access to the shared folder by clicking the original sharing invitation link.
- If a participant of a shared folder deletes a sub-folder or file within that shared folder, that sub-folder or file deletes from all participants' devices, and recovery is not available.

If you're worried about losing a file, be sure to keep a local copy in addition to the shared copy in iCloud Drive. Learn more about deleting files in iCloud Drive and how to recover deleted files on iCloud.com.

* If Recently Deleted doesn't restore your files as expected, you can sign in to iCloud.com, click Account Settings, and under Advanced, click Restore Files. If you empty your Trash or use Delete All in Recently Deleted, you can't recover your files.

The emphasis is mine, but I added it because—Holy Mother of Baby Bovines!—that's not OK! Apple has basically just said that anyone you add to an iCloud Drive shared folder can delete the entire contents of a shared folder and you can't do anything about it. Bad Apple!

But wait, it gets worse. After the discussion with Paul, I got busy and put off writing up the problem. When I went back to our conversation today and clicked the link he had sent me, I ended up on a different page that focused on sharing iCloud Drive files and folders using iCloud.com. This page said nothing about what happens if a participant of a shared folder deletes a file or folder.

The new page threw me for a loop, but as is so often the case with Web shenanigans, the Internet Archive's Wayback Machine revealed what had happened. Sometime between March 21st and April 1st, Apple started redirecting the previous

page to the new one. Some spelunking through Apple's documentation revealed that the company had split the previous page, which covered iCloud Drive sharing in iOS, macOS, Windows, and iCloud.com, into standalone pages in the macOS User Guide and iCloud User Guide. Yet another page that I found only through a search—it wasn't linked to the pages about iCloud Drive folder sharing—discussed file and folder deletion, but without the emphasized warning from before:

If you're a participant who can change shared files: Deleting a file from a shared folder deletes it from everyone's devices.

Delete shared folders or files in iCloud Drive

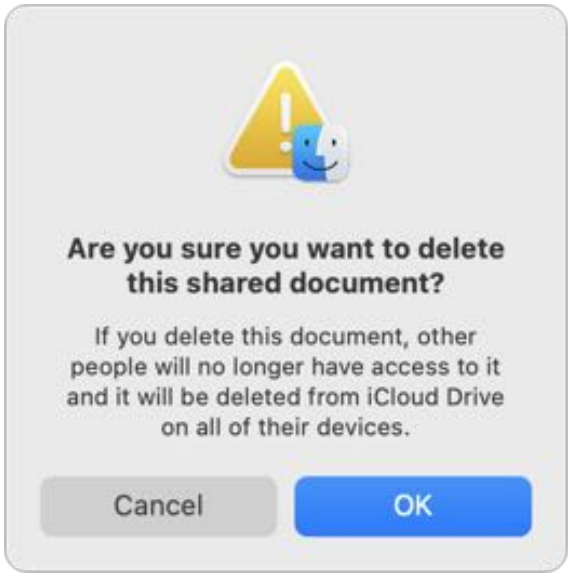
1. In iCloud Drive on your Mac, drag the folder or file to the Trash, then confirm that you want to delete the item.
2. Do one of the following:
   - *If you're the owner:* The folder or file is removed from the devices of everyone you shared it with.
   - *If you're a participant who can change shared files:* Deleting a file from a shared folder deletes it from everyone's devices. Deleting a shared folder removes it from your devices, but not from the owner's devices or the devices of other participants.

   You can access the folder or file again using the original link sent by the owner, unless the owner stopped sharing the folder or file.

With Hanlon's Razor in mind, I think it's unlikely that Apple intended to bury the fact that iCloud Drive shared folders are susceptible to data loss when participants delete files or folders from within a shared folder. Regardless of why it happened, the fact remains that Apple went from merely hiding this fact in a long but appropriate document to putting it in the bottom of a locked file cabinet stuck in a disused lavatory with a sign on the door saying "Beware of the Leopard." Bad Apple!

But Maybe It's Not True Anymore?

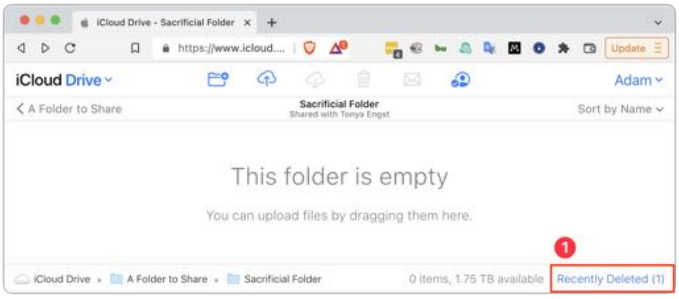
There's another possibility. Perhaps Apple fixed iCloud Sharing shared folders so that files deleted by participants aren't deleted with no chance for recovery? Wouldn't that be great? Don't get your hopes up.

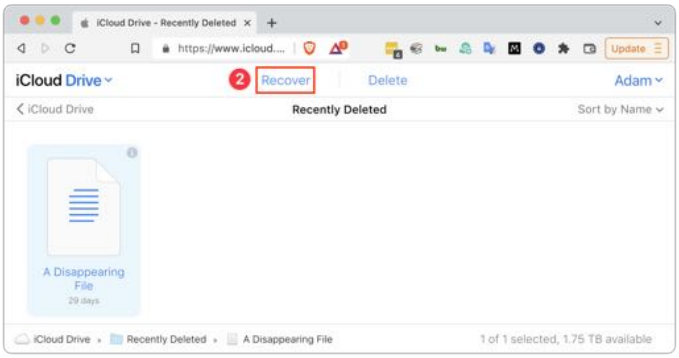


To test, I put a test file in an iCloud Drive folder I share with Tonya, and we watched the file appear on her MacBook Pro. Then she deleted the file, which presented a warning dialog. At least Apple warns sharing users that deleting a file will take it away from others in the shared folder. What Apple doesn't say is that deleting a file in an iCloud Drive shared folder does **not** result in that file being moved to the local Trash as you would expect from decades of using the Finder. Instead, macOS deletes the file instantly, which, while prefaced with a warning, is terrible behavior for a cloud sharing service. Bad Apple!

Why would Apple leave such a glaring hole in iCloud Drive folder sharing? After all, if the owner of a shared folder deletes a file in that folder, macOS and iCloud Drive provide the expected opportunities for recovery. When I deleted another test file from my shared folder, I saw the same warning dialog as Tonya, but the file ended up in my local Trash, from which I could easily restore it. Plus, when I logged into iCloud.com and looked in iCloud Drive, a Recently Deleted link appeared in the lower-right corner ❶. Clicking that link revealed the equivalent of iCloud Drive's trash. Selecting the file and clicking Recover ❷ extracted the file from my local Trash and restored it to the sub-folder from which I had deleted it. With files deleted by

the owner, iCloud Drive is doing everything right.





You might think that if Tonya, as a sharing participant, were to add a file to my iCloud Drive shared folder and then delete it, it would be treated as an owner-deleted file and end up in her local Trash. You would be wrong. Files added to the shared folder by participants are equally at risk for immediate deletion as any other. Bad Apple!

It's worth noting that moving a file out of an iCloud Drive shared folder to another location on the Mac has the same effect of taking the file away from others who have access to the shared folder. Apple provides a similar warning dialog in that scenario, but the major difference is that the file remains available to whoever moved it out of iCloud Drive, such that they could put it back.

How Much Should We Worry?

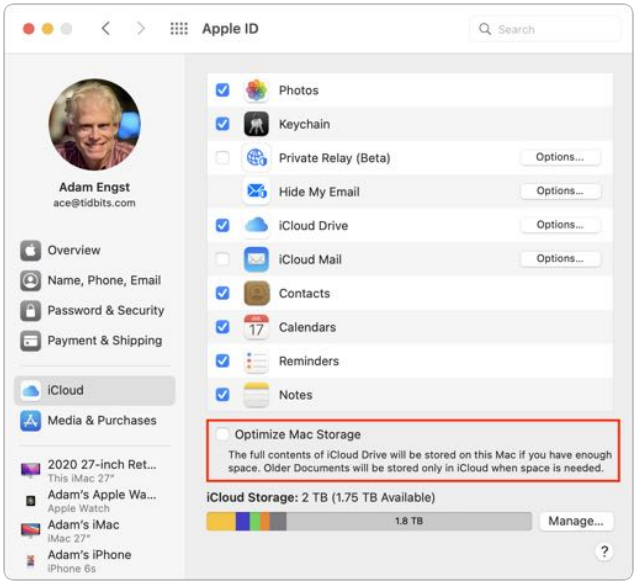
iCloud Drive folder sharing has been around since macOS 10.15 Catalina, so it's no longer new, and Apple has had two major releases of macOS to address underlying issues if they couldn't be addressed entirely on the iCloud side. That hasn't happened, which could suggest that Apple doesn't see the immediate deletion of files by sharing participants as a problem. Or perhaps Apple's engineers think that the warning dialog is sufficient. I'd push back hard on that—a keyboard-focused user who's moving quickly could delete a file with Command-Delete and press Return to dismiss the dialog before even reading it.

I haven't used iCloud Drive folder sharing in a fast-paced collaborative work environment, so I can't speak from direct experience, but over 14 years of coordinating Take Control work in Dropbox, files occasionally went missing and needed to be restored from Dropbox's Deleted Files collection. In a workflow that requires regular trashing of temporary files, it's easy to imagine accidental deletion of more important documents. Plus, you're at the mercy of everyone with whom you've shared an iCloud Drive folder. Are they all sufficiently technical and alert that they would never make a mistake? The other major cloud sharing services all offer such a purgatory for deleted files along with version history capabilities to protect against accidental editing or corruption—iCloud Drive sticks out like a sore thumb here.

Luckily, there is one bright spot in this otherwise bleak picture of iCloud Drive folder sharing, not that Apple will tell you about it: Time Machine. By default, Time Machine backs up the local copies of iCloud Drive files, not just for the owner, but also

for all participants. I confirmed that Tonya's Mac had backups of all the files in our shared folder, and I could click through the dates in Time Machine and see the contents of that folder change appropriately.

You'll notice that I was careful to say that Time Machine backs up the *local copies* of iCloud Drive files. If you have Optimize Mac Storage selected in System Preferences > Apple ID > iCloud, macOS might replace iCloud Drive files with local stubs, and those stubs, even if backed up, wouldn't contain the data you want. So, if you're using iCloud Drive folder sharing, make sure to deselect Optimize Mac Storage or, if you need to keep that on due to insufficient local storage space, get someone else in your sharing group to do so. That's your last-ditch backup if someone inadvertently deletes an important file.



Despite this hidden Time Machine workaround, Apple has done a poor job here. In the modern world, there should be no easy way to delete data, particularly someone else's data, without any option for recovery. A single warning dialog with a default OK button that means "Nuke This File From Space" is unacceptable. For goodness sake, Apple popularized the entire concept of multi-step file deletion! Move a file to the Trash, choose Finder > Empty Trash, and respond affirmatively to the prompt—that's been a staple of Mac use since 1984. Preventing accidental data loss is table stakes.

The solution to this particular problem is conceptually simple. Any file deleted or removed from an iCloud Drive shared folder by a participant should be treated just like a file deleted or moved by the owner. It may be technically simple as well. If you open your iCloud Drive folder in the Finder and press Command-Shift-. to reveal hidden files and folders, you'll see a hidden .Trash folder (press Command-Shift-. a second time to hide them again). iCloud Drive files you delete as the owner go into that folder, which presumably causes them to appear in the local Trash and in the iCloud Drive Recently Deleted folder. Why can't shared files deleted by a sharing group participant go into their .Trash folder, appear in their local Trash, and trigger a notification to the owner or the rest of the group?

If you want to encourage Apple to step up and make iCloud Drive folder sharing work correctly, give feedback to the iCloud engineers.

By Adam Engst

Another Step Toward a Password-Free Future

Put bluntly, passwords suck. We just published a lengthy article about an email scam that exists only because too many people have weak passwords that they reuse across multiple sites (see "How to Help a Friend Whose Email Has Been Hacked to Send Scams," 5 May 2022). Why don't we instead get to use sophisticated biometric authentication like Touch ID and Face ID more broadly? That may

happen in the coming year, thanks to Apple, Google, and Microsoft committing to support the FIDO standard for passwordless logins.

To an extent, all three companies already support FIDO Alliance standards to enable passwordless logins, but this announcement expands those capabilities by providing automatic access to FIDO passkeys on multiple devices without having to re-enroll every account and by allowing FIDO authentication on a mobile device to sign in to an app or website on another device nearby, regardless of the operating system or Web browser in use.

Last year at Six Colors, Dan Moren wrote about Apple's Passkeys system, introduced as a technology preview at WWDC 2021. It gives a glimpse of how Apple thinks this new passwordless authentication approach will work. In short, when you sign up for an Internet account, you would create only a username; Passkeys would create the passkey and store it in your keychain. All the Internet service would have is your username and your public key. When you want to sign in later, all Passkeys would have to do is prove that your device has the corresponding private key, which it would do by asking you to authenticate via Touch ID or Face ID. That would raise questions about how users would deal with the loss of a device and seemingly eliminate the possibility of signing in using someone else's device, but those are implementation details.

With luck, we'll start to see Passkeys (or whatever Apple ends up calling it) implemented for real in the upcoming releases of macOS 13, iOS 16, iPadOS 16, and watchOS 9. As the press release says:

These new capabilities are expected to become available across Apple, Google, and Microsoft platforms over the course of the coming year.

It can't happen soon enough. Death to passwords!

By Adam Engst

How to Help a Friend Whose Email Has Been Hacked to Send Scams

Beware of an email-based scam that's making the rounds this year! Since January, I've been targeted three times, and I wanted to share the story—both to help you avoid falling prey to the scam and so you can better alert any friends or acquaintances whose email accounts have been hacked.

First, let me bang the drum one more time: None of these people would have had problems if their email passwords had been strong and unique. If you reuse your email password anywhere, or if it's short and obvious, stop reading right now and *go change it*.

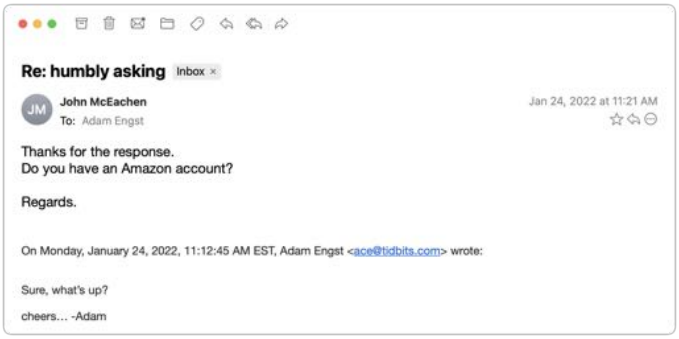
Your new email password can be at least 13 truly random characters (something like iR82dGlQf3&@C) or at least 28 characters of common words separated by hyphens (like the classic correct-battery-horse-staple), or you could generate it through some combination of numbers (like dates) and letters (such as initials) that make sense to you. Whatever you choose, it must be strong and unique. And if you're not using a password manager, you're wasting your time and likely being insecure.

How the Scam Progresses

The email scam message I received came from someone I know quite tangentially—John is a

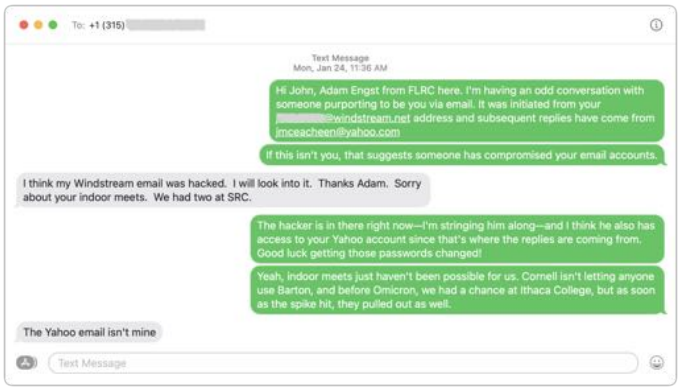
runner from a nearby city who had participated in some of the track meets that I organize. Since I assign bib numbers and announce all the races, his name was sufficiently familiar that I wasn't surprised to receive email from him—we had corresponded once in 2021 about an upcoming track meet. But with only one prior conversation, I had no sense of his email style, so his first message didn't raise any alarm bells in my head.

I replied generally to the first message—there were various reasons an upstate New York runner might contact me—but those alarm bells went off instantly upon receiving the next message.

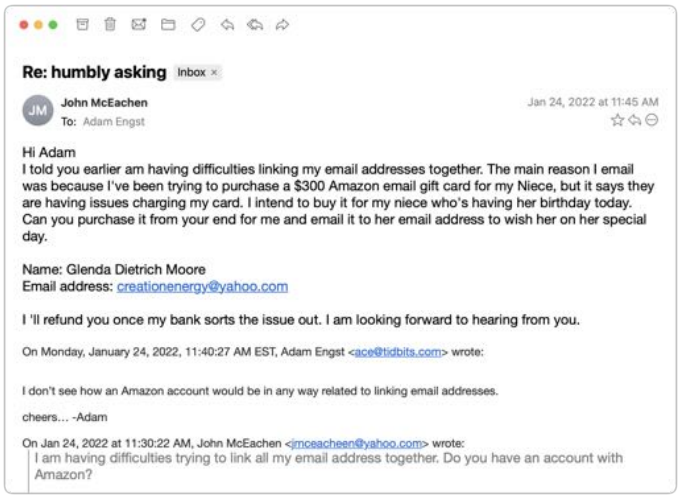


I couldn't see any reason why a person I barely knew would ask if I had an Amazon account, and besides, at this point, who doesn't? I switched into investigation mode. What you can't tell from the message above is that although the sender's name remained the same, the email address had changed from windstream.net to yahoo.com. Combined with the strange request about an Amazon account, I was now nearly certain I was talking to a scammer who was using the email address switch to get me into their own account in case John locked them out by changing his password. I decided to keep the scammer talking and see what I could learn.

After sending that message, I looked up John's phone number in his most recent track meet registration and texted him. Luckily, I was able to provide sufficient context in my initial text that he knew who I was. As I expected, he knew nothing about what was happening and confirmed that the Yahoo account wasn't his.

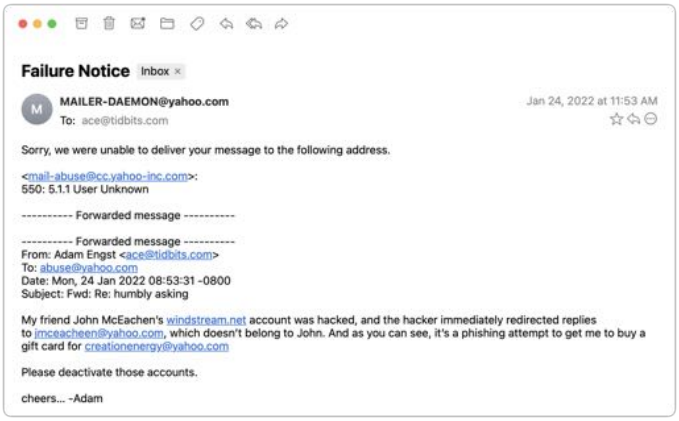


By now, I was curious what the scam would be, so I kept pretending that I was skeptical but still going along with it all. After another message or two, it became clear—the scammer wanted me to buy a $300 Amazon gift card for which they would reimburse me later. Yeah, right.

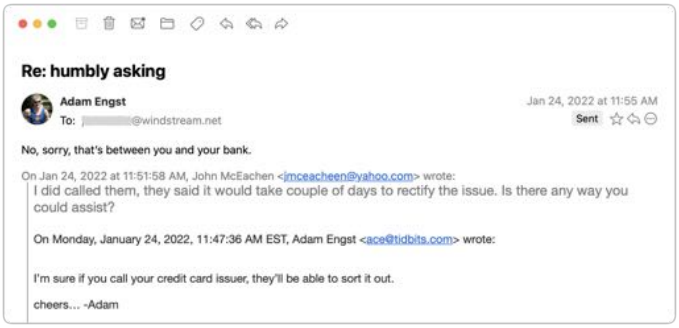


Throughout all this, I made sure to send only to the windstream.net account in part to see if the scammer would lose access. I was simultaneously keeping up the text backchannel with John, who said that he saw none of these messages in his Sent mailbox nor messages from me in his Inbox, which suggested that the scammer was somehow deleting them instantly to cover their tracks. I assume that John changed his password, but if so, that apparently didn't kick the scammer out because I kept getting replies to the messages I sent to windstream.net.

I entertained a faint hope that Yahoo would be interested in shutting down both the scammer's address and the address they wanted me to use for the Amazon gift card. But no, my attempt to alert abuse@yahoo.com failed. I subsequently tried to contact Yahoo via a recommended Web form after I mentioned the issue in "Yahoo-Backed POP Connections Cause TidBITS Formatting Error" (26 January 2022), but that was equally unsuccessful.



By this time, I had traded a few more messages with the scammer to keep the conversation going, but they eventually gave up on me. I never heard back again after this message.



I didn't get around to writing up this story right away and quickly forgot about it. But a month later, it happened again! Vern isn't someone with whom I've ever exchanged email, but he runs an excellent U-Pick blueberry farm in my nearby hometown, and I had left my email address in his visitor book the last time I picked berries there. Luckily, I had an in for contacting him—my father used to be the mail carrier, and he still knows most people in town. Dad was able to call him and let him know about the problem, and Vern changed his password and alerted all his email contacts not to reply to the scam messages. Amusingly, this time, Vern's real email address was at Yahoo, and the scammer was trying to redirect replies to a fake Outlook account.

Two months later, the scam reappeared in my email, with the scammer victimizing an older runner in the area. In this case, I'd been talking about Tom with another friend who worked with him regularly just the day before, so I recruited my friend to encourage Tom to change his password.

How to Help Your Friends

Let's assume that you get one of these messages. They're so weirdly generic that you'll realize it's a scam right away if they come from someone you know well. Or, as in the case of my second example, you'll know the person so slightly that the scam will be obvious purely because a stranger would never ask such questions. The awkward middle occurs if the message is like my first and third examples, where I knew the people just well enough that I wasn't surprised to get email from

them but not well enough to be certain that the message was fake.

Nevertheless, if you're unsure, there's no harm in replying—just don't get sucked in! If you notice that your reply (or any subsequent one) is going to an address other than where the first one originated, that's another clue that you're in the middle of a con. Once you realize what's going on, here's what I recommend doing… and not doing:

- **Do recommend a password change:** By calling, texting, or emailing a secondary address, tell the person whose account has been hacked to change their email account password immediately and recommend that they create a strong, unique password using a password manager. You must assume that the scammer has full control over the victim's primary email account and will delete all warnings and evidence of wrongdoing.
- **Do encourage alerting of other contacts:** Although the person whose account was hacked probably won't be able to tell who received the scam message, encourage them to alert all their contacts that the previous message was fake and should be ignored. Also, suggest that they encourage their contacts to check their passwords—might the acquaintances of people whose passwords were so weak as to be compromised be likely to have weak passwords as well?
- **Don't fall for the scam:** Never buy an Amazon or other gift card for someone you don't know just because they ask. (If you want to give someone money, become a TidBITS member.)
- **Don't mark it as spam:** Don't mark the initial message from the scammer as spam or report it as phishing. Remember, it's essentially legitimate email, having been sent from the compromised account, so marking it as spam could cause future real messages from that person to be filtered too.
- **Don't bother reporting the scammer:** Sadly, I don't recommend trying to report the scammer to whatever email service they're using. The goal is good, but it's all too likely to be a waste of your time.

To make it easier to alert victims, here's a sample message you can text them or use as a script when talking to them:

I*t looks like your email account has been hacked and used to send scam messages to contacts like me. I'd encourage you to change your email password immediately, making the new password strong and unique, ideally using a password manager app. Also, it would be good to alert your contacts to ignore the scam message and encourage them to make sure their own passwords are secure.*

Finally, if you have friends who aren't Internet-savvy, share these stories so they have a better chance of avoiding being scammed or having their accounts compromised.

Apple Updates

Security Update 2022-004 (Catalina)
May 16, 2022 — 1.6 GB

System Requirements

– macOS 10.15

macOS Catalina Security Update 2021-004 (19H1922) is recommended for all users and improves the security of macOS.