

printout

Keystone MacCentral Macintosh Users Group ♦ www.keystonemac.com

Keystone MacCentral June 17th 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

 Apple Notes Continued



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 April Meeting	1
Apple Operating Systems Jump to 26?	3
From iPhone to AI By Adam Engst	3 - 4
VPN Use Is Widespread	4 - 8

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 © 2025, 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

Treasurer

Tim Sullivan

Program Director

Dennis McMahon

Membership Chair

Eric Adams

Newsletter Editor

Tim Sullivan

Web Master

Tom Bank II



Apple Operating Systems Jump to 26?

Mark Gurman of Bloomberg reports that Apple will switch its

operating system version numbering scheme from the current mess to identifying them by years. It's about time. 🕒

By Adam Engst

From iPhone to AI: Why Jony Ive's OpenAI Deal Signals a Power Shift

In a video dripping with so much mutual admiration that I found myself muttering “Get a room,” former Apple designer [Jony Ive and OpenAI CEO Sam Altman have announced a collaboration](#) to “create a family of devices that would let people use AI to create all sorts of wonderful things.” Ive’s hardware design company, io Products, will be [acquired by OpenAI for \\$6.5 billion in stock](#), despite having only 55 employees and never having shipped anything. Ive and his team will oversee creative and design aspects across all OpenAI products, including ChatGPT and other apps.

Despite all the self-congratulatory Bay Area tech bro exaggeration, the announcement is not pure fluffery. ChatGPT—and generative AI overall—is arguably one of the most transformative technologies since the Internet and the smartphone.

It’s hard to envision what we’ll use to interact with AI in the future besides the smartphone, smartwatch, and earbuds we have today. Jarringly—and perhaps tellingly—despite the video being staged as an informal discussion in a San Francisco coffee shop, Altman chose to describe current usage of ChatGPT in a laptop browser instead of the ChatGPT app on a phone.

The next piece of AI hardware won’t be the now-defunct [Humane AI Pin](#) (which also had investment from Sam Altman and a partnership with OpenAI) or the [Rabbit r1](#) (which Marques Brownlee described as “[barely reviewable](#),” after calling the Humane AI Pin “[the worst product I’ve ever reviewed](#)”). It’s certainly not the Apple Vision Pro, which, remember, is a “spatial computer.” It may eventually be glasses, even if the [Ray-Ban Meta AI Glasses](#) haven’t set the world on fire.

Years of hearing overblown promises have made me inherently skeptical, but Jony Ive and his team have done important work in the past, and OpenAI has the resources and the chutzpah to bring a product to the mainstream market. [Whatever it is](#), it’s slated for late 2026.

Regardless of what OpenAI ultimately ships, this announcement may signal a shift in the balance of power in the tech world. Jony Ive, the guy who played a key role in designing iconic products like the iMac, iPod, iPhone, and MacBook, is now focused on creating the next generation of consumer technology for OpenAI rather than Apple.

Meanwhile, instead of making the iPhone the preferred platform for AI, Apple has struggled to develop and implement a compelling AI vision. At best, Apple Intelligence is currently a scattershot

collection of unimpressive features that barely change the user experience; at worst, it's a promised version of Siri that's hard to imagine living up to its marketing. Even more embarrassingly, [Perplexity has released a version of its voice assistant](#) on iOS that encroaches on Siri's territory by linking a modern chatbot to public APIs that enable it to create reminders and events, load inline maps, play songs from Apple Music, and more.

Perhaps we shouldn't be surprised. Apple's cultural DNA is built around perfecting individual, on-device experiences instead of fostering social interactions, community development, and engagement with the broader Internet. Consider features like [iTunes Ping](#), [Game Center](#), and [Apple Music Connect](#), which struggled due to closed ecosystems, limited opportunities for interaction, and insufficient attention and resources. Apple has also failed to compete in the blogging and publishing space, having discontinued [iWeb](#), limited iCloud sharing to specific data types, and

kept Pages focused on print output. And, of course, there's search, where Apple has consistently depended on Google and other partners to provide information to Spotlight and Siri rather than creating its own index.

Apple's desire to limit its engagement with the messiness of the Internet isn't just a historical curiosity—it may represent an existential threat to the company's future. Recently, in the Google antitrust case, Apple's senior vice president of services, Eddy Cue, speculated that “you may not need an iPhone 10 years from now” as technology evolves, particularly due to AI. He also noted that AI-powered search features, such as I wrote about in “[AI Answer Engines Are Worth Trying](#)” (17 April 2025), have contributed to [Safari searches declining](#) for the first time in 22 years.

So Apple executives recognize the threat. The question is, can they generate the youthful perspectives, energy, and enthusiasm needed to keep Apple relevant?

By Adam Engst

VPN Use Is Widespread Do You Use It?

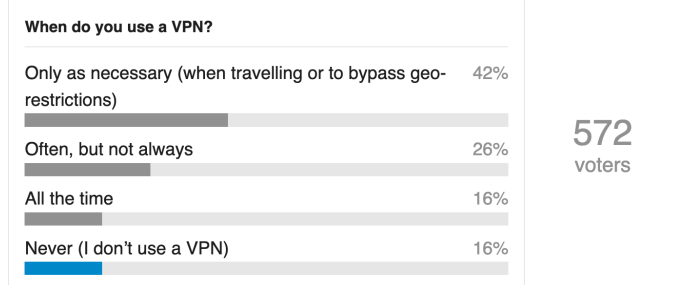
Prompted by the latest revelations about common VPNs being owned by Chinese companies that may share data with their government, our latest Do You Use It? poll explored how TidBITS readers use VPNs. As someone who has never used a VPN, I was surprised by their popularity—84% of respondents use one at least some of the time. As always, the results of this poll reflect the audience and shouldn't be interpreted to imply anything more broadly.

Before we start, let's make sure we're all on the same page. A VPN, or virtual private network, is low-level software that enhances your privacy and security by routing your Internet traffic through an

encrypted tunnel to a remote server, hiding it from potential attackers on your local network or between you and the destination. Many people also use VPNs to circumvent location- and IP-based restrictions that support geographic content licensing and the desires of organizations to block certain types of content.

When Do You Use a VPN?

We started the poll by asking when people use a VPN to assess the overall level of VPN usage. The distribution of responses was fascinating, with the all-or-nothing answers bookending the results at 16% each. In the middle, 26% of participants indicated they often use a VPN, while 42% rely on one only when necessary.



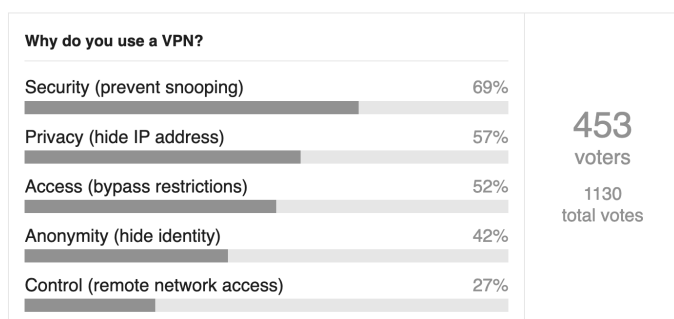
Only 16% of respondents never use a VPN, which may reflect the technical aptitude and security-mindedness of TidBITS readers. I can't speak for others, but I've never found the need to use a VPN because I work from home nearly all the time. Most of my traffic is already encrypted with HTTPS, I don't download torrents or engage in activities where I'm concerned about protecting my privacy from my ISP, and I don't watch videos or do other things that run afoul of geo-restrictions.

The 16% of respondents who use a VPN all the time seemed to fall into two categories: those who are required to do so by their employer (and see no reason to turn the VPN off for personal work) and those who are willing to endure a bit of inconvenience for complete privacy protection.

That inconvenience seems to be what causes 26% of respondents to turn off their VPNs occasionally. People mainly reported performance issues and difficulties with websites not loading or functioning properly when accessed via a VPN. These issues undoubtedly influence why 42% of respondents say they use a VPN only when necessary. In other words, VPNs don't just work for everyone.

Why Do You Use a VPN?

Our next question attempted to discern what those who do use VPNs aim to achieve.



The answers require some unpacking:

• **Security (69%):** The most common reason people use a VPN is to ensure security—they want a guarantee that no one can eavesdrop on their connection and read data. Organizations care deeply about confidential information, which is one reason employers often mandate VPN usage. The risk of an attacker connected to the same public Wi-Fi network being able to see unencrypted traffic also drives many people to use VPNs when working outside the home or office. While added security is generally beneficial, it's important to remember that most Internet traffic is now encrypted by default. Nearly all Web pages use HTTPS, most email over IMAP and SMTP employs TLS encryption, everything transmitted via iMessage is encrypted, and so on. The primary unencrypted traffic for most individuals consists of DNS lookups, which reveal which websites you are visiting, even if the actual data transferred remains encrypted.

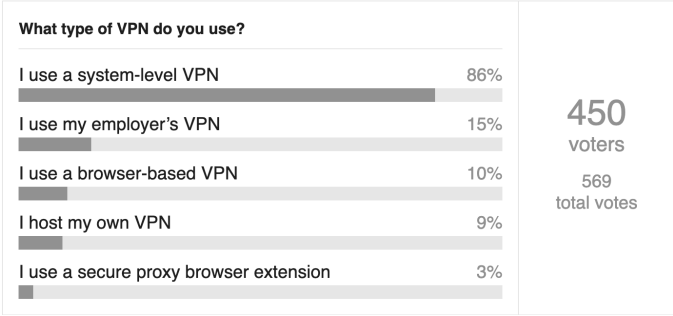
• **Privacy (57%):** The next most common issue is privacy, or controlling who sees what you do, which directly relates to the fact that most DNS traffic isn't encrypted. When you use a VPN, neither your ISP nor an attacker on the same local network can determine where you're going and thus infer what you're doing. However, the VPN provider can see that information and may log it, potentially allowing it to be exposed, at least to law enforcement. Remote websites see an IP address, but it's that of the VPN server, not your ISP or device, which may also enhance your privacy.

• **Access (52%):** Another major reason TidBITS readers use a VPN is to bypass access restrictions. Streaming services may have licenses to show content in some countries but not in others, sports teams may have streaming blackouts in their local markets, and so on. With a VPN, you can make your traffic appear to originate from an allowed location. Given the ease and popularity of circumventing these arbitrary restrictions, one would hope they will diminish over time. VPNs also assist people in working around organizational restrictions, such as schools blocking games or employers limiting access to adult sites.

- **Anonymity (42%):** This answer was higher than I expected, which may have been due to people conflating it with privacy and voting for both. I was trying to tease out VPN use triggered by the desire to be completely anonymous—to make it difficult or impossible to connect your online activity back to who you are. A VPN contributes to that—selecting one that doesn’t log traffic is crucial—but you must also limit your actions to avoid leaving clues about who you are.
- **Control (27%):** The least common reason for using a VPN was control, by which I meant remote network access. Two prominent examples include accessing network resources on an employer’s network—such as file servers and printers—and connecting to your home network while traveling. Several people mentioned using Tailscale to access their home networks, as Glenn Fleishman described in “Tailscale Gives You Remote Access to Your LAN from Anywhere” (24 February 2025).

What Type of VPN Do You Use?

One of the complications of this poll is that precisely what constitutes a VPN is somewhat unclear. The initial trigger for the poll was to warn people about potentially problematic Chinese VPNs and seek recommendations for alternatives, but that didn’t account for enterprise-grade VPNs used by large organizations or individuals hosting their own VPNs. As I delved deeper into the topic, I discovered that there are also browser-level VPNs that protect only Web traffic, along with secure proxy browser extensions that provide much the same functionality through other protocols. Some browser-based VPNs are actually secure proxies as well. It’s quite a mess, so the next question asked what type of VPN you use.



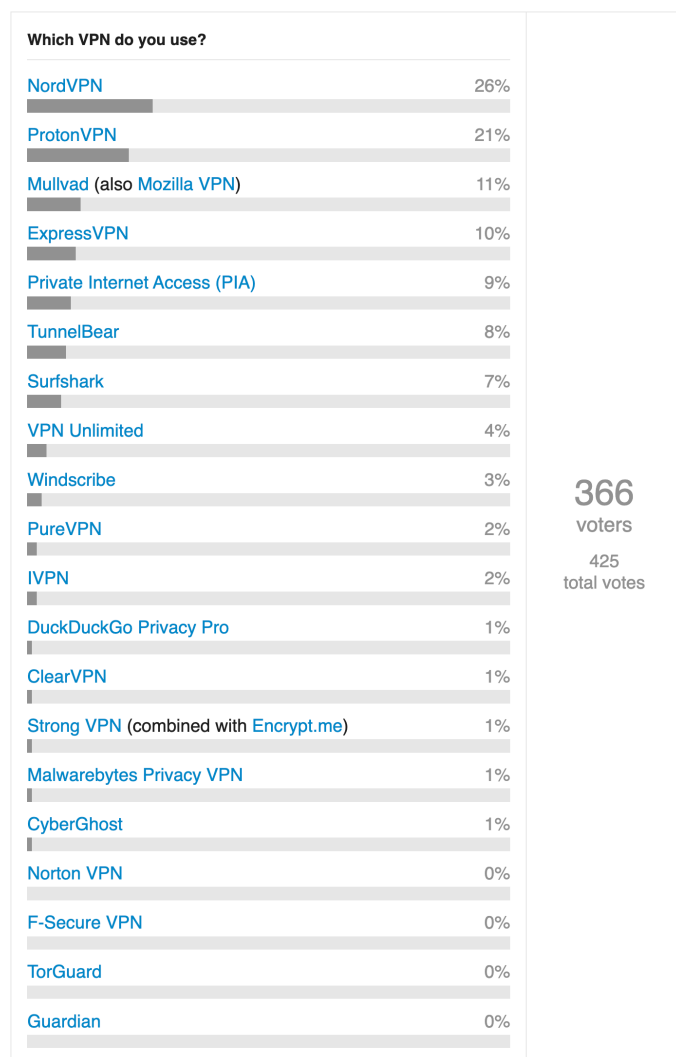
The answers offered some clarity:

- **System-level VPN (86%):** Most respondents rely on a system-level VPN that protects all the traffic leaving the computer. To my mind, that aligns closely with what most people consider a VPN to be—an encrypted tunnel for everything.
- **Employer’s VPN (15%):** I suspect that most of those who use their employer’s VPN also voted for the system-level VPN, as enterprise VPNs manage all traffic. This figure also aligns fairly well with the 16% of respondents who use a VPN all the time.
- **Browser-based VPNs (10%):** These VPNs are relatively new, which may explain the low ranking for this answer. Opera introduced the concept in 2016 with a secure proxy, but the full-fledged Brave VPN (based on Guardian) only launched in 2020, and the similarly functional Proton VPN for Vivaldi came out this year.
- **Self-hosted VPN (9%):** It’s too much work for most people to host their own VPN. I suspect that many people responding with this answer were referring to Tailscale, although there are certainly approaches using dedicated software or hardware.
- **Secure proxy browser extension (3%):** Very few people use these browser extensions, which I think is generally a good thing because many of those I looked at seemed a little sketchy.

Which VPN Do You Use?

Our final question aimed to identify the most popular VPNs among TidBITS readers. While some readers suggested alternatives in the comments—our polls max out at 20 answers—I doubt any would have received significant

votes. Therefore, anyone looking for a VPN should consider the top-rated choices below.



While I can't provide personal recommendations, a few notes are warranted for the responses garnering more than 5% of the votes:

- **NordVPN (26%):** The most popular choice was NordVPN, which features a welcome option to disable itself on trusted networks. However, a reader reported encountering difficulties while traveling in China, although he didn't specify whether he attempted different VPN protocols, some of which are more easily detected and blocked. Several users noted receiving poor tech support, with one individual unable to get it

to function on his iPhone. Prices range from \$3.39 to \$12.99 per month, depending on the plan and length of subscription.

- **Proton VPN (21%):** Proton VPN was almost as popular. No one had anything negative to say about the service, although there were questions about whether it was worth the price, which seems comparable to others. There appears to be a 70% off deal right now, causing prices to range from \$2.99 to \$9.99 per month.
- **Mullvad/Mozilla VPN (11%):** I combined these products into one answer because Mozilla VPN uses Mullvad's servers. Several people noted that Mullvad also integrates with Tailscale, allowing you to route Internet-bound traffic through Mullvad's servers while keeping local traffic within the Tailscale network. Mullvad charges a flat rate of €5 per month, regardless of how long you subscribe—that's currently \$5.69 in US dollars. In contrast, Mozilla VPN costs \$4.99 or \$9.99 per month, depending on billing frequency.
- **ExpressVPN (10%):** While one user said he had found ExpressVPN to be the best for bypassing geo-restrictions (the streaming services try to block VPN connections for obvious reasons), others raised concerns about the company's ownership. ExpressVPN was acquired in 2021 by Kape Technologies, a British holding company that also owns Private Internet Access (next) and CyberGhost (1%), along with the antivirus company Intego and a review site that ranks Kape's companies highly. Kape was previously known as Crossrider and was associated with adware. ExpressVPN's monthly prices range from \$4.99 to \$12.95.
- **Private Internet Access (9%):** As with ExpressVPN, only one person mentioned using Private Internet Access, presumably

successfully. Again, Private Internet Access is owned by Kape Technologies, which some may consider a negative. Its prices range from \$2.03 to \$11.95 per month.

- **TunnelBear (8%):** Several respondents expressed their fondness for TunnelBear, mentioning that it is operated by Plucky Canadians™ and complimenting its Web login screen of a cartoon bear covering its eyes with its paws while a password is being typed in. One individual remarked that he had found it slow several years ago. TunnelBear's pricing ranges from \$3.33 to \$9.99 per month.
- **Surfshark (7%):** While it continues to operate independently, Surfshark merged with Nord Security, the company behind NordVPN, in 2022. No one commented about it, and its monthly pricing ranges from \$1.99 to \$15.45.

While I still find the VPN space overwhelming, if I needed to use a VPN, I would start by investigating NordVPN, Proton VPN, Mullvad, TunnelBear, and Surfshark. I find Mullvad's flat-rate pricing attractive for short-term usage, although in that case, I would probably also consider whether Brave VPN or Proton VPN for Vivaldi would meet my needs. But that's just me. If you're trying to compare these or other VPNs, Randy Singer shared a link to the CyberInsider site, which has reviewed and compared many of the VPNs. Wirecutter recommends Mullvad, TunnelBear, and Proton VPN.

I remain comfortable not using a VPN, but I wouldn't judge anyone who did. 🐻

