



An International Association of Technology & Computer User Groups

Our Club

RCSI is a nonprofit 501(c)(3) group open for membership to anyone interested in computers and new technology. Established in 1981, our aim is to provide an exchange of information between users of digital devices. We are not in any way affiliated with any computer manufacturer or software company, and **we do not sell your data or email address.**

Program Meetings

No admission fee for non-members. Everyone is welcome! Second Tuesday of every month, **except July and August**, from 6:30pm-8:30pm.

Help's Half Hour (Q & A) 6:30pm – 7:00pm. *Members and Guests are welcome to attend and bring their computer related questions with them to get answered. Yes, you may bring the problem computer with you.*

7:00 – 7:15, Club Business

7:15 – 8:30+, Main Presentation
Come and join in the fun and enjoy a snack! **You are welcome to bring a guest.**

Become a Member

The club would like to have you as a member, and your subscription will help to keep us going. Go to our website, www.rcsi.org, and download a printed form for use by the Post Office mail, **or** enter your info online and pay with a credit card or PayPal, **or** attend a meeting.

The Rochester Computer Society, Inc. a computer/tech club open to everyone



Vol. 43, No.5 web: www.rcsi.org Rochester, NY May, 2024

**May 14, 'Alternative Energy Sources', Arpad Kovacs
'Personal Home Robots', Tony Dellelo
June 11, "Human-Computer Interaction",
"What are Chiplets", "Latest Tech Products"**

In This Issue

How Can Passkeys Possibly Be Safe?	Leo Notenboom
DuckDuckGo Now Has a Privacy Subscription	Arol Wright
Investigating the new Macbook Air M3	Faheem A Zaidi
Bits and Pieces in the News	RCSI editor
Take it From the Rats	
AMD Announces Ryzen Pro 8000 CPUs	
Club and Regional News	
Harmful 'forever chemicals' Removed from Water	UofR

How Can Passkeys Possibly Be Safe?

Mostly because there's nothing to steal.

by Leo Notenboom, <https://askleo.com/>
Making Technology Work For Everyone

Passkeys may feel confusing now, but they're a doorway to a more secure, less frustrating, passwordless future.

(Image: DALL-E 3)

There's still a fair amount of discomfort around the concept of passkeys as replacements for passwords. The most common objection is something like "So if someone has access to my machine, don't they have access to all my accounts?"



“Your Computer User Group of the Air”, Saturdays from 12:00 pm to 2:00 pm, with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM (WGMC) from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415, www.jazz901.org
Sound Bytes is the longest running computer call-in show in the known universe.

We have stopped printing the Monitor newsletter. Digital copies can be emailed or obtained from www.rcsi.org or my Pcloud storage at <https://tinyurl.com/tonydel-rcsi> (this link works in PDF version only). Also includes presentation slides, **past newsletters dating back to 1996** and articles too large for this newsletter.

- Some Past Presentations:**
- Autonomous Cars and Robots
 - Open Source and Free Software
 - Protecting Your Identity
 - Tablets, the Programs and Uses
 - Personal Finance Software
 - Amazing Browser Tips
 - Linux is Like Cars
 - Drones and Their Many Uses
 - Gifts and Gadgets for the Holidays
 - Cut the Cord, Streaming Services
 - 3D Printing, ENABLE project
 - Features, Mac OS X & Windows
 - The New Space Race, 2021
 - Tech of South America
 - Internet Security and Privacy
 - AI and Digital Assistants
 - Emerging Technologies
 - My Favorite Android Apps

The answer, of course, is more complicated than a simple yes or no. The important thing to realize, though, is that passkeys actually add a layer of security.

Passkeys & safety

Passkeys are a secure authentication method stored on specific devices that require user verification through mechanisms like Windows Hello. They enhance security by enabling passwordless sign-in and keep you safer by eliminating common vulnerabilities associated with traditional passwords and other authentication mechanisms.

What Is a Passkey?

Passkeys are a new form of authentication that promise to be both easier and more secure.

In short, passkeys are digital keys assigned to a specific device by a one-time authorization process. This process may involve one or more other authentication mechanisms associated with your account. These may include:

- Password authentication
- One-time codes sent to email
- One-time codes sent to a phone
- One-time codes from an authenticator smartphone app
- Authorization on an already-signed-in device
- A one-time [backup](#) access code created when the passkey or [two-factor authentication](#) is enabled

Once set up, passkeys are stored securely on each machine and require you to authenticate each time they are used, typically via Windows Hello PIN, fingerprint, or facial recognition, or possibly with your Windows sign-in password.

By default, passkeys are valid only for the machine on which they’re set up. The only exception is that some password managers now also act as secure passkey repositories, allowing a passkey to be stored and used wherever that password manager is used. Once again, additional confirmation is required each time a passkey is used, either in the form of Windows Hello or by entering your password manager’s master password.

Hello?

Windows ‘Hello’ is another poorly named feature of Windows. It’s a technique of using either a PIN or biometrics to sign in to Windows. It’s something you enable on each machine. PINs, if used, are unique to each machine, and, of course, your biometrics are unique to you.

Because PINs and biometrics are quick, easy, and secure, Windows Hello is often used as a layer of additional authentication when you’re about to do something that requires extra security.

Like using a passkey.

APCUG, An International
Association of Technology and
Computer User Groups

<https://apcug2.org/>

Saturday Safaris

Exploring Technology in Depth
Saturdays:
12 pm – 2 pm EST

<https://apcug2.org/saturday-safaris/>

Tech for Seniors

[https://
www.techforsenior.com](https://www.techforsenior.com)

hosted by Ron Brown
and Hewie Poplock
Every Monday from 9-10 AM PT,
(12-1 PM ET)

Broadcast with Zoom
The meeting ID is **526-610-331**
(there is no password) and you'll
be placed in a waiting room and
then admitted.

#

APCUG Website Help

Windows & Android Tips:

By Judy Taylour

[https://apcug2.org/
jerestips/](https://apcug2.org/jerestips/)

Apple Tech Tips:

[https://apcug2.org/50-best-
mac-tips-tricks-timesavers/](https://apcug2.org/50-best-mac-tips-tricks-timesavers/)

Penguin Platform (Linux):

[https://apcug2.org/
penguin-platform/](https://apcug2.org/penguin-platform/)

Chromebook Tips And Tricks:

[https://apcug2.org/
chromebook-tips-and-
tricks/](https://apcug2.org/chromebook-tips-and-tricks/)

Signing in

Responses to Your Three Common Password Manager Objections

Password vaults are a common recommendation by security professionals to improve your online security. Why do so many resist?

Let's compare the different ways we might sign in to an online account.

Sign in using a password only

When only passwords are used, you manually enter your username and correct password to gain access.

Sign in using a password from a password vault

Using a password vault, you unlock your vault either with its master password or Windows Hello. The vault fills in your sign-in credentials for you or makes them easily available to copy/paste. Password vaults are more secure than manually entering passwords because they enable long, complex passwords without ever re-using a password.

Sign in using a passkey only

The first time you sign in to an account using a passkey, you'll be asked to authenticate yourself using one of the secondary methods listed above. Once authenticated, the passkey is created and saved to Windows' secure storage. This is repeated for each machine you use.

The next time you sign in on that specific machine, you'll be presented with Windows Hello PIN or biometric authentication. That's the passkey being used to sign you in.

Sign in using a passkey from a password vault

Using passkeys saved in a password vault, the first time you sign in to an account using passkeys on *any* machine, you'll be asked to authenticate yourself using one of the secondary methods listed above. Once authenticated, the passkey is created and saved to your password vault.

The next time you sign in on any machine on which you use that password vault, you'll be presented with Windows Hello PIN, biometric authentication, or your password vault's master password prompt. Once confirmed, you're signed in. The passkey will have been used to sign you in.

Practical applications of passkeys

Let's examine the reality of using passkeys in two scenarios. The first one people ask about frequently: someone walks up to your machine, and because your passkeys are activated, do they have access to your accounts? The second — when your computer is infected with [malware](#) — is one people don't ask about as much but I think is more important.

RCSI Board Members

President:

Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com

Treasurer:

Jerry Seward
jerry@jerryseward.com

Members-At-Large:

Bob Avery 385-4491
Webmaster
webmaster@rcsi.org, 9/24

Jan Rothfuss 347-6020
Membership & Help's Half Hour
jan_rothfuss@hotmail.com, 9/26

Tony Dellelo 734-6149
Programs & Monitor editor
tonydel@techie.com, 9/25

Got Questions?:

Windows: Arpad Kovacs
podcomputer@gmail.com

Linux & some Mac:
Carl Schmidtman
unixgeek@faultline.com

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, * * ONLINE * *. We will be using Zoom. ANY CLUB MEMBER MAY ATTEND.

Monitor Newsletter

The Monitor is published monthly by members of RCSI. Articles by our members may be reprinted by other user groups or nonprofits, without special permission. A courtesy copy may be emailed to the author or Monitor editor. Limited copies (probably in black and white) will be printed and available at our meetings.

Club Mailing Address

Rochester Computer Society, Inc
PO Box 18516
Rochester, NY 14618

Scenario #1: Someone walks up to your computer

First: Is this a likely scenario?

First, let's consider how likely or unlikely this scenario is for you. How often do people you don't trust have access to your computer? If it's never or rare, then this isn't an issue. This scenario doesn't apply to you, and you don't need to worry about it.

Second: if the machine is signed out, locked, or turned off, the attacker needs your sign-in credentials. That could mean your password or your Windows Hello PIN. Without those, none of these scenarios apply. You're done. They don't have access to anything on the machine.

Now, if someone a) has physical access to your machine, **and** b) you leave your machine unlocked, as many of us do, then this scenario may come into play.

Here's what's required to sign in to one of your online accounts by someone who just walks up to your unlocked machine.

If you use passwords only

They need to know your username and password for each account. If they have that, naturally they can sign to any account and use it as you.

If you use a password from a password vault

If the vault is locked, then:

- They need to know your password vault's username and master password...
- Or they need to be able to authenticate via Windows Hello if your vault is configured to use it.
- They may also need your two-factor key or code if your vault is configured to require it.

Without any of that, they can't get in.

But what if you leave your vault unlocked? This is one of the reasons I recommend an auto-lock timeout in your password vault. If people can walk up to your machine, make it short. If it's not really an issue but you still want to protect yourself, choose something longer. Since I have Windows Hello enabled in 1Password, I have it configured to lock after four hours (Windows Hello quickly unlocks) and require my full master password once every 30 days (and after rebooting).

If they get in, not only can they sign into whatever account they like, but of course they can run off with the contents of your vault, allowing them access to your accounts from elsewhere later.

If you use passkeys only

They need to know your Windows Hello PIN or your Windows password. (Theoretically, having your face or fingerprint would also work if you're using biometrics.)

Tidbits of probably useless information

You might think that your nostrils share the workload when it comes to taking in oxygen. Instead of both taking in the same amount of air when you breathe, you actually inhale most of your oxygen through [one nostril at a time](#). Every few hours, the active nostril will take a break and the other one will take over until they ultimately switch back again.

The human brain is responsible for countless tasks and is always busy keeping our internal systems running. In order to remain so vitally productive, [the brain uses 20 percent of both the oxygen and the blood](#) in your body, according to Healthline.

It's a well-known fact that ravens are wildly intelligent creatures. But 2019 research published in the journal *Proceedings of the National Academy of Sciences* discovered that the birds are also very in tune with the feelings of the creatures around them. This [empathetic trait](#) had previously only been observed in primates.

In 2015, researchers from the University of Vienna gathered 947 hours of [giraffe noises](#) over an eight-year period at three zoos and they discovered that the animals produced a humming sound at night. The scientists hypothesize that the animals do this to help keep their herd together when their vision is impaired in the low light.

If they have those credentials, they could sign in to your passkey-protected accounts, but *only from that machine*. There is nothing to steal and nothing they can take to their own machines.

If you use passkeys from a password vault

If the vault is locked, then:

- They need to know your password vault's username and master password,
- Or they need to be able to authenticate via Windows Hello if your vault is configured to use it.
- They may also need to use or have your two-factor key or code if you have your vault configured to require it.

In addition, when attempting to use a passkey stored in the vault, they will *again* be required to authenticate themselves with either Windows Hello PIN or your vault's master password.

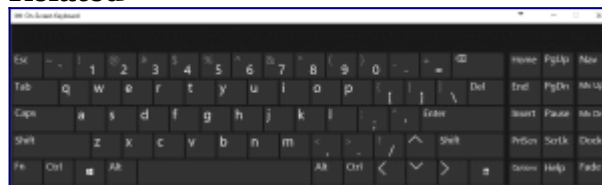
If they compromised your vault, then they can, of course, export everything — *except the passkeys*. Passkeys cannot be stolen. In addition, if your account is passwordless — requiring either a passkey or one of your backup authentication methods to sign in — they have no password to steal and thus cannot access the account. [1](#)

Scenario 2: Malware on your machine

What I consider to be a more likely and important scenario that people don't ask about as much is when there is malware on your machine. How do passkeys relate to malware?

Malware can do anything, so we have to control what it can find. This is where passkeys really shine.

Related



[Will Using an On-Screen Keyboard Stop Keyloggers?](#)

Using an on-screen keyboard instead of a real keyboard might stop some keyloggers, but there's no guarantee that other techniques aren't also being used.

If you use passwords only

Malware containing a [keylogger](#) can slurp up your sign-in credentials.

If you use passwords from a password vault

Malware containing a keylogger can slurp up your sign-in credentials to any online account you sign in to and possibly to the password vault.

8 WAYS TO KEEP YOUR LAPTOP BATTERY HEALTHY FOR A LONG TIME

— Most laptops nowadays are powered by lithium-ion batteries, also called Li-ion batteries. While these batteries can hold a full charge when new, they gradually lose this capacity over time. Taking proper care of them is crucial to preserve their ability to hold maximum charge for as long as possible, and here are some tips to help you do just that. Read more at [8 Ways to Keep Your Laptop Battery Healthy for a Long Time \(makeuseof.com\)](#)

MICROSOFT COPILOT CONTINUES TO IMPROVE, GAINING 3 NEW POPULAR PLUGINS — HERE'S WHAT THEY ARE AND HOW TO USE THEM

— While overall ChatGPT adoption seems to be high, especially in an enterprise setting, Copilot doesn't seem to have hit the mass market appeal that ChatGPT has. This difference is likely due to lagging in useful features. Today Microsoft took a step to remedy that, while not as exciting as GPTs in the GPT store for ChatGPT, application plugins for Copilot are a good step in the right direction. For more about the plugins, read this Windows Central article.

[Copilot now features plugins for some awesome applications | Windows Central](#)

If you use passkeys only

There is nothing for malware to capture. Passkeys cannot be intercepted.² The malware cannot sign in to your online account.

If you use passkeys from a password vault

If the password vault also uses passkeys for authorization, then there is nothing for malware to capture. The malware cannot sign in to your online account or your vault.

Passkeys significantly increase your protection from malware.

Going Passwordless

One of the interesting side-effects of passkeys, and, I suspect, one of their goals, is that they are more secure than passwords. In fact, if your account has a password at all, it's ever-so-slightly less secure than a passwordless account using passkeys or any other authorization mechanisms.

Why? Because when alternative mechanisms are used exclusively, there's no password to steal. There's nothing to be caught by a keylogger, nothing to be guessed, and nothing to be exposed in a [breach](#).

For example, medium.com accounts have no password. To sign in, you provide an email address, and they send a code or link to that email address. Your ability to receive that email and act on it gives you access to the site. There's no password involved.

Passkeys make going passwordless much more convenient. Once set up, instead of waiting for an email, you simply respond to Windows Hello asking you for a PIN or biometric, and you're done.

[Security: It's a Spectrum, Not a State](#)

Many people want to be secure, not realizing there's no such thing.

[Im]Perfect Security

“Yeah, but Leo, what about this scenario....???”

Whenever I discuss security — particularly account authentication techniques — I always get pushback from folks with scenarios that a) they don't believe I addressed, and b) they believe make the entire argument moot because the perception of what they've “discovered” is so severe.

Sometimes I learn something. I love when that happens.

More often than not, though, it just points out that I didn't explain a [core](#) concept properly, because that severe scenario is not only covered but covered well by the technology.

The other scenario is when they're absolutely, positively, right, but what they're right about is such an implausible scenario that it's not worth getting worked up about.

There is no such thing as perfect security. You cannot *be* secure. You can only be more secure or less secure.

Scams

By AARP

Voiceprint Scams

Thanks to technological advances, it's possible for thieves to capture a recording of your voice and then use a software program to generate an imitation "deepfake" version that can be used to impersonate you. "That voiceprint can be used to access your insurance or your financial institution or apply for a driver's license," Bruemmer says. The New York Times reported on a recent case in which a representative at a major bank received a call from a deepfake copy of a Florida investor's voice, requesting that the bank move the man's money elsewhere. Fortunately, the fraud attempt was spotted by the bank before the real investor lost his savings.

Delayed-action sweepstakes scam

[Sweepstakes scammers](#), who call or write to say that you've won a fabulous fortune, have been around for ages. But recently they've come up with a new variation on the old formula, according to Bruemmer. Instead of trying to get you to pay taxes or other fees in advance to collect the nonexistent prize, the scammers will ask for personal information so that they can validate you and set up the payout. "They'll say, just give us your banking information and your Social Security number, and we'll file with the IRS and we'll take care of everything," he explains. They'll write small checks on your account to see whether you notice the fraudulent activity.

Passkeys help you become significantly more secure.

Do this

While unrelated to the above, my #1 tip for account security is to use [two-factor authentication](#).

Then start getting familiar with passkeys. Enable it on one of your accounts (Google's a good choice) and get a feel for how it works. I suspect you'll find it quite convenient. I know you'll be seeing it more and more.

Then consider making one of your accounts passwordless. Microsoft rolled this out some time ago. You'll find the option in the security settings for your Microsoft account.

And finally, consider having your password vault store passkeys for you so you can take them from machine to machine. The reward for all of it is more freedom and fewer passwords.

From Leo's website: <https://askleo.com/how-can-passkeys-possibly-be-safe/>.

Looking for more security tips and safety nets? [Subscribe to Confident Computing!](#) Less frustration and more confidence, solutions, answers, and tips in your inbox every week.

From the <https://askleo.com/> website.

* * * * * SOFTWARE and HARDWARE * * * * *

DuckDuckGo Now Has a Privacy Subscription

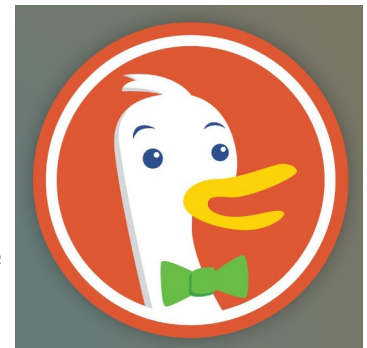
By [Arol Wright](#), 4/11/24

Three privacy-focused services in one duck-branded package.

DuckDuckGo started out as a more private alternative to search engines like Google and Bing, but the company has slowly expanded to browser extensions, web browsers, and other tools. DuckDuckGo is now going one step further with a new "privacy subscription" that aims to keep you protected across the internet.

[DuckDuckGo](#) has just announced a new subscription service called "Privacy Pro."

It's not one single service, but rather three new privacy protections that the company is lumping into one single convenient package. You get access to an anonymous VPN for secure connections on up to five devices simultaneously, Personal Information Removal to combat identity theft by removing personal details from data broker sites, and Identity Theft Restoration services to assist in recovering from identity theft incidents. With all three, you can stay anonymous while online and also work against any potential damage that might actually happen.



Virtual Tours

Ashford Castle, Ireland
Built in 1228, this County Mayo castle was transformed into a luxury hotel in the 1930s. One of the most [beautiful castles in Europe](#), Ashford has hosted a number of celebrity weddings and frequently draws the rich and famous. It's also served as the setting for the classic film starring John Wayne, "The Quiet Man." Guests today can enjoy living out their castle fantasies with a stay in one of the sumptuous rooms adorned with antique furnishings, some with open fireplaces, clawfoot tubs and four-poster beds. While it's not possible at the moment, you can take a [virtual tour](#) and perhaps plan a dream trip in the future.

Palace of Versailles, France is one of the most popular attractions in France, Chateau de Versailles, or the Palace of Versailles is one of the most stunning examples of [royal residences](#) from the 17th and 18th-century in the world. Google Arts & Culture has created a famous collection from the famous home of King Louis XIV, the country's king from May of 1643 until his death in 1715, that can be marveled at via an especially impressive [virtual tour](#). In addition to exploring the palace, you can check out some of its best artifacts, take a virtual stroll through the gardens and head inside the famous Hall of Mirrors.

Privacy Pro's VPN ensures secure internet connections without logging user activity. It encrypts connections across devices and hides users' locations and IP addresses from websites and ISPs. The service, built on the WireGuard protocol, automatically reconnects if the connection is interrupted. DuckDuckGo also claims to not collect any logs, saying on its website, "we don't have any record of website visits, DNS requests, IP addresses connected, or session lengths."

Personal Information Removal scans and removes personal data from people search sites, reducing the risk of identity theft. Unlike other services, it only initiates removal requests after confirming the presence of user data in broker databases and stores user information locally for privacy. Finally, Identity Theft Restoration offers support in the event of identity theft incidents. Services include credit repair, document replacement, travel assistance, and reimbursement for certain expenses associated with restoration.

How much does this bundle cost, then, you might ask? These three things are available for you for a mere \$9.99/month or \$99.99/year. While currently limited to United States residents, expansion to other regions is planned for the future. That's not cheap, and there's a lot of competition. There are countless options for [VPN services](#), and there are a few personal data removal services, including [the Mozilla Monitor Plus subscription](#) that launched back in February.

You can check out [DuckDuckGo's website](#) for more information.

INVESTIGATING THE NEW MACBOOK AIR M3: STOCKPILING AND SPEED EXPERIENCES

By Faheem A Zaidi, Pakistan, April 5, 2024

INVESTIGATING THE NEW MACBOOK AIR M3: STOCKPILING AND SPEED EXPERIENCES

The MacBook Air M3, disclosed by Macintosh, has been causing disturbances in the tech world, promising amazing execution upgrades and huge enhancements away capacities. In this article, we dig into the complexities of the MacBook Air M3's stockpiling and speed highlights, investigating how they add to the general client experience.

Grasping the Meaning of Stockpiling and Speed in Workstations

In the present quick moving computerized scene, the significance of capacity and speed in PCs couldn't possibly be more significant. Capacity limit directs how much information a client can store on their gadget, going from reports and photographs to applications and media documents. Then again, still up in the air by the processor and capacity innovation, impacts the responsiveness and effectiveness of the PC.

The Benefits of Strong State Drives (SSDs)

Current PCs, including the MacBook Air M3, regularly highlight Strong State Drives (SSDs) rather than customary Hard Circle Drives (HDDs). SSDs offer a few benefits over HDDs, including quicker read

Interesting Internet Finds

Samsung Air Dresser-

Minimize trips to the dry cleaner with the Samsung Air dresser designed to deodorize, sanitize while getting rid of the wrinkles. [Samsung.com](https://www.samsung.com)

Most refer to the Internet as a goldmine of knowledge but it also happens to be one of the best places to kill time.

ChatGPT has taken the internet by storm unless you're living under a rock. The AI chatbot developed by OpenAI is set to revolutionize how we use the internet. ChatGPT is one of the best websites to kill time in 2024. You can ask the AI chatbot about anything and be ready to be surprised by the answers. [Www.chat.openai.com](https://www.chat.openai.com)

Drench is one browser game that's sure to help you kill hours in one go. In Drench, you get a board full of different colors and you have to 'drench' the entire board in one single color. The challenge is that you only get a limited number of turns to finish the board, so you have to think carefully about how you'll proceed with the objective. <http://www.flashbynight.com/drench/>

If AI and deep-fakes fascinate you, this website generates fake people using GAN (or generative adversarial networks) and displays them to you. You can refresh the page to see a different face. <https://thispersondoesnotexist.com/>

and compose speeds, lower power utilization, and improved sturdiness because of the shortfall of moving parts. These advantages mean faster boot times, snappier application dispatches, and generally smoother execution.

An Outline of the MacBook Air M3's Stockpiling Choices SSD Capacity Limits

The MacBook Air M3 is accessible in different SSD stockpiling setups, going from humble limits appropriate for easygoing clients to bigger choices taking care of experts with requesting stockpiling needs. Apple offers choices going from 128GB to 1TB, permitting clients to pick the limit that best lines up with their use prerequisites.

Examination with Past MacBook Air Models

Contrasted with its ancestors, the MacBook Air M3 flaunts critical enhancements away execution and productivity. The reception of quicker SSDs adds to decreased stacking times for applications and improved performing multiple tasks capacities, guaranteeing a consistent client experience.

Examining the Speed Execution of the MacBook Air M3 Processor Proficiency

The MacBook Air M3 is controlled by Macintosh's hand crafted M-series processors, famous for their outstanding exhibition and power proficiency. The combination of cutting edge chip design empowers the MacBook Air M3 to convey great speed and responsiveness, whether taking care of regular errands or escalated responsibilities.

Benchmark Correlations

Benchmark tests led on the MacBook Air M3 exhibit its ability in taking care of requesting errands effortlessly. The blend of high velocity SSD stockpiling and effective processor execution brings about quick application dispatches, smooth performing various tasks, and responsive client cooperations, setting another norm for execution in the ultraportable PC class.

Genuine Ramifications: What Stockpiling and Speed Mean for Client Experience

In genuine situations, the capacity and speed abilities of the MacBook Air M3 mean unmistakable advantages for clients. From consistent substance creation and altering to quick information moves and smooth mixed media playback, the MacBook Air M3 enables clients to achieve errands with proficiency and accuracy, improving efficiency and imagination.

Ways to augment MacBook Air M3 Execution

To enhance the presentation of the MacBook Air M3, clients can utilize different techniques, including routinely refreshing the working framework and applications, overseeing extra room productively, and using worked in streamlining devices, for example, macOS's Stockpiling The board highlight. Moreover, limiting foundation processes and using outer capacity arrangements can additionally upgrade the MacBook Air M3's presentation and life span.

*** * Jokes & Quotes Stolen
from Everywhere * ***

Revenge:

Three rough-looking bikers stomp into a truck stop where a grizzled old-timer is having breakfast.

One of the bikers extinguishes his cigarette in the old guy's pancakes. The second biker spits a wad of chewing tobacco into his coffee. The third biker dumps the whole plate onto the floor.

Without a word of protest, the old guy pays his bill and leaves.

"Not much of a man, was he?" says one of the bikers.

"Not much of a driver, either," says the waitress. "He just backed his truck over three motorcycles."

My second wife left me because I have "revenge issues"
We'll see about that...

Unbelievable!!! My girlfriend broke up with me yesterday, so in revenge I stole her wheelchair...

Well, guess who came crawling back today...

This girl I used to go out with is still using my Netflix Account, and that is cool. She's watching Scandal and is currently on S7E12. Season finale is S7E18. Guess who is changing her password as soon as she gets to S7E17?

As Revenge For My Brother Wrapping My Christmas Present In Duct Tape Last Year, This Year I've Wrapped My Brother's Present In Concrete! Revenge Best Served Stone-Cold

Future Assumptions: Likely Improvements Away and Speed Innovation

As innovation keeps on developing, we can expect further headways away and speed innovation, prompting considerably quicker and more productive PCs. Developments, for example, PCIe 4.0 SSDs, high level chip designs, and computer based intelligence driven advancement calculations hold the commitment of opening new degrees of execution and efficiency in later cycles of the MacBook Air and other ultraportable workstations.

All in all, the MacBook Air M3 addresses a critical jump forward with regards to capacity and speed abilities, offering clients a convincing mix of execution, proficiency, and flexibility. With its fast SSD stockpiling, effective processor, and smooth plan, the MacBook Air M3 rethinks the guidelines for ultraportable PCs, engaging clients to achieve more effortlessly.

Note about the author: I Faheem a Zaidi from Pakistan . I am a professional writer and I writing since 25 years, My article continue publishing in Pakistani biggest magazine.

*** * * * * BITS and PIECES in the NEWS * * * * ***

Editor's Note: To continue reading the following articles, you may copy the long URL at the end of the article and enter it into a web browser **or** click on the URL in the PDF or web versions of this newsletter.

Take it From the Rats: A Junk Food Diet Can Cause Long-Term Damage to Adolescent Brains

University of Southern California, News Release 15-Apr-2024

Rats that were fed a diet chock-full of fat and sugar in their adolescence suffered memory impairment, USC researchers found.

A new USC-led study on rats that feasted on a high-fat, sugary diet raises the possibility that a junk food-filled diet in teens may disrupt their brains' memory ability for a long time.

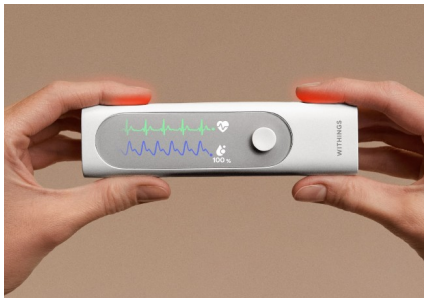
"What we see, not just in this paper, but in some of our other recent work, is that if these rats grew up on this junk food diet, then they have these memory impairments that don't go away," said Scott Kanoski, a professor of biological sciences at the USC Dornsife College of Letters, Arts and Sciences. "If you just simply put them on a healthy diet, these effects unfortunately last well into adulthood."

The study appears in the May issue of the journal [Brain, Behavior, and Immunity](#).

In developing the study, Kanoski and lead author and postdoctoral research fellow Anna Hayes considered that [prior research](#) has shown a link between poor diet and Alzheimer's disease. People who suffer from Alzheimer's disease tend to have lower levels of a neurotransmitter called acetylcholine in the brain that is essential for

Odds and Ends

We're still a long way from carrying a Star Trek-style tricorder with us, but the [Withings BeamO](#) might just be the first step. This small handheld device — about the size of a stubby highlighter — is capable of measuring your body temperature and blood oxygen saturation, provides medical-grade ECG readings, and serves a digital stethoscope for monitoring heart and lung functions.



According to Withings, the BeamO can pick up signs of atrial fibrillation (AFib), blood oxygen desaturation, heart murmurs, asthma, COPD and more, and then share those results with a healthcare professional via your smartphone. Users can even stream their stethoscope audio directly to a doctor during telehealth appointments. While Withings is still waiting for FDA approval, it hopes to ship the device by the summer. — *Mike Prospero*

memory and functions such as learning, attention, arousal and involuntary muscle movement.

The team wondered what this could mean for younger people who may be on a similar fat-filled, sugary Western diet, particularly during adolescence when their brain is undergoing significant development.

Kanoski emphasized that adolescence is a very sensitive period for the brain when important changes are occurring in development. “I don’t know how to say this without sounding like Cassandra and doom and gloom,” he said, “but unfortunately, some things that may be more easily reversible during adulthood are less reversible when they are occurring during childhood.”

There is at least some hope for intervention. Kanoski said that in another round of the study, the research team examined whether the memory damage in rats raised on the junk food diet could be reversed with medication that induces the release of acetylcholine. They used two drugs, PNU-282987 and carbachol, and found that with those treatments given directly to the hippocampus, a brain region that controls memory and is disrupted in Alzheimer’s disease, the rats’ memory ability was restored.

Reported in <https://www.eurekalert.org/news-releases/1041331>.

AMD Announces Ryzen Pro 8000 CPUs With Improved AI Performance

By [Josh Norem](#) April 16, 2024

AMD has added its AI-boosting NPU to the newest line of desktop and mobile CPUs for business users.

The Ryzen 8000 Pro chips for desktops and mobile devices are launching today. AMD promises improved [AI performance](#) for business users thanks to a newly added neural processing unit (NPU). The company directly targets Intel with this launch, as business users have always heavily favored Intel’s processors. However, AMD says its solution is superior in performance and efficiency, even when compared with Intel’s newest Meteor Lake chips.

The [company is launching](#) two new chip families today: the Ryzen 8000 Pro for desktops and the Ryzen Pro 8040 series for mobile users. AMD has added its NPU to both chip families (for the high-end chips), which it says will give business users better on-device AI performance. This is apparently a crucial new requirement for this class of machines, as companies don’t want to use the cloud for AI due to privacy concerns. Using AI in this scenario includes chatbots, image generators, and office apps.

Although both families are still Zen 4 CPUs, AMD has upgraded them from the 7000-series process

of TSMC 5nm to TSMC 4nm, [according](#) to PCMag. It has also changed



the name to Ryzen AI Pro versus Ryzen Pro for its predecessors. AMD is launching eight new mobile and desktop processors, and AMD says it'll help businesses safely deploy AI to its road warriors and desktop jockeys alike with better performance and efficiency than what Intel (and Apple) are offering.

Overall, this is another salvo in the long-simmering "AI PC" battle. AMD and Intel are ramping up their efforts in this space and have begun focusing much more on AI performance instead of traditional benchmarks to show a chip's performance. AMD says these chips will go into pre-made computers from companies like Lenovo and HP starting in Q2, so right now essentially.

Found on <https://www.extremetech.com/computing/amd-announces-ryzen-pro-8000-cpus-with-improved-ai-performance>.

CLUB and REGIONAL NEWS

Harmful 'forever chemicals' Removed from Water with New Electrocatalysis Method

[Luke Auburn](#), March 5, 2024

A novel approach using laser-made nanomaterials created from nonprecious metals could lay the foundation for globally scalable remediation techniques.

Scientists from the [University of Rochester](#) have developed new electrochemical approaches to clean up pollution from “forever chemicals” found in clothing, food packaging, firefighting foams, and a wide array of other products. A new [Journal of Catalysis study](#) describes nanocatalysts developed to remediate per- and polyfluoroalkyl substances, known as PFAS.

The researchers, led by assistant professor of chemical engineering [Astrid Müller](#), focused on a specific type of PFAS called Perfluorooctane sulfonate (PFOS), which was once widely used for stain-resistant products but is now banned in much of the world for its harm to human and animal health. PFOS is still widespread and persistent in the environment, despite being phased out by US manufacturers in the early 2000s, continuing to show up in water supplies.

“Using pulsed laser in liquid synthesis, we can control the surface chemistry of these catalysts in ways you cannot do in traditional wet chemistry methods,” says Müller. “You can control the size of the resulting nanoparticles through the light-matter interaction, basically blasting them apart.”

“I would argue that in the end, a lot of decarbonization efforts—from geothermal heat pumps to efficient refrigeration to solar cells—depend on the availability of PFAS,” says Müller. “I believe it’s possible to use PFAS in a circular, sustainable way if we can leverage electrocatalytic solutions to break fluorocarbon bonds and get the fluoride back out safely without putting it into the environment.”

Check it out at <https://www.rochester.edu/newscenter/pfas-chemicals-in-water-electrocatalysis-method-596532/>.

Got Questions?

Send an email to either person below and they will get back to you. The questions can be related to the OS (Operating System) or hardware related issues. Please give them time for a response, as they do this service on a volunteer basis. Thank you.

Windows OS: Arpad Kovacs, podcomputer@gmail.com

Linux & some Mac: Carl Schmidtman, unixgeek@faultline.com

Our Meeting Place

St John's Meadows at

Johnsarbor Drive, is on the left, past Clinton Avenue, when going West on Elmwood Avenue. The opening in the white fence is Johnsarbor Drive. At the “T”, turn right. The meeting is in the SECOND building on the left –

Chestnut Court.

Our meeting place can change. Please check our website before each meeting. **www.rcsi.org**