DTS DanTech Services
Computers under control!™

Technology Times February 2023 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problem? - Click Here!

Considering an app to manage your passwords? This advice will be key no matter which app you choose.

By Rob Pegararo

Right before Christmas, LastPass left out an unwelcome present for users of its password-manager service: a Dec. 22 update to a "Notice of Recent Security Incident" post reporting that the unknown attackers behind a breach the company first revealed in August had managed to "copy a backup of customer vault data."

This data now at risk includes web addresses, usernames and passwords for saved logins. But with the last two remaining encrypted, the post advised LastPass users not to panic because the attackers would need either extraordinarily good luck or an extraordinarily long amount of time to unlock any one vault by trying random passwords, one after another.

"Because of the hashing and encryption methods we use to protect our customers, it would be extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices," CEO Karim Toubba wrote in the post.

Are password managers easily hacked?

- Continued on page 4

One Windows compatibility hold could block updates on some devices

Microsoft has started the forced rollout of Windows 11 22H2 to systems running Windows 11 21H2 that are approaching their end-of-support (EOS) date on October 10, 2023. Redmond is regularly initiating automatic feature updates to ensure that it can continue to service these devices near their EOS date and to provide them with the latest updates, security updates, and improvements. The automated feature update rollout phase comes after Windows 11 22H2 (known as the Windows 11 2022 update) has also become available for broad deployment today to users with eligible devices via Windows Update.

"Today we begin to automatically update consumer and non-managed business devices running Windows 11, version 21H2 Home and Pro editions to Windows 11, version 22H2," Microsoft said in an update to the health dashboard. "Since Windows 10, we have been helping Windows users stay up to date and secure with supported versions of Windows through automatic updates. We are utilizing this same approach for Windows 11 to help you stay protected and productive."

The automatic updates will roll out gradually, starting with the devices running Windows 11 21H2 for the longest time. "If you are interested in moving to Windows 11, version 22H2 right away, open Windows Update settings and select Check for updates. If your device is ready, you will see the option to Download and install,"
Microsoft added today.

"If we detect that your device might have an issue, such as compatibility, we might put a safeguard hold in place. In this case, the update will not be installed automatically until the issue is resolved." Right now, the only compatibility hold blocking the Windows 11 2022 Update affects systems with specific driver versions for Intel Smart Sound Technology (Intel SST) on Intel 11th Gen Core processors that trigger blue screens of death (BSODs).

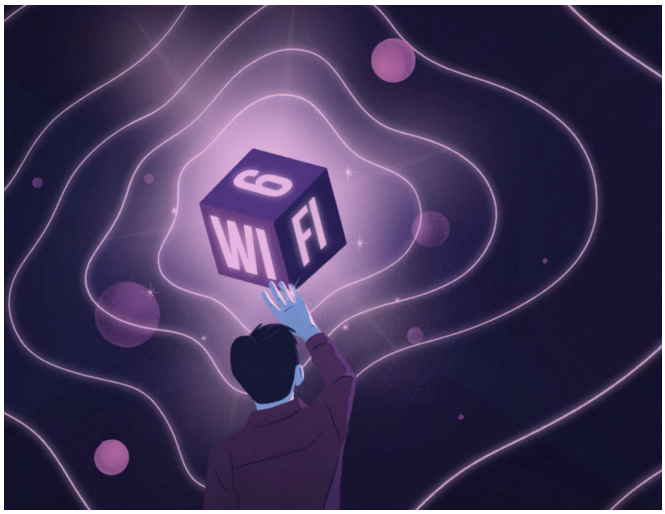
However, Microsoft provides a workaround for those who want to install Windows 11 22H2, requiring them to check if Intel has an updated driver for their systems. The issue is resolved by updating the Intel SST drivers to version 10.30.00.5714 and later or 10.29.00.5714 and later.

After updating the affected Intel driver, it can take up to 48 hours before you can install the Windows 11 2022 Update on your system. You can use this Windows support document or follow this guided walk-through to troubleshoot Windows 10 22H2 update problems or fix any errors you encounter.

What Is WiFi6 and How Can It Help Your Business?

The newest iteration of wireless technology, called WiFi6, is starting to become increasingly popular in the business world. This technology provides powerful performance improvements and increased range compared to its predecessors. Business owners who want to stay ahead of the curve should think about investing in WiFi6 for their operations.

WiFi6 is capable of providing dramatically improved range, speed, and battery life compared to earlier versions of Wi-Fi technology. It also has improved capacity for handling multiple devices connected at once without sacrificing performance or speed. This makes it ideal for businesses that need reliable wireless access throughout their facility or office space—especially if they have many employees who are all connected at the same time.



One of the biggest advantages offered by this new version of wireless technology is its raw speed. With current standards like 802-11ac offering maximum speeds of up to 867 Mbps on a single connection, WiFi6 can provide speeds up to 4x faster than its predecessor—with peak speeds reaching up to 3.5 Gbps on a single connection (depending on the device). Thats more than enough bandwidth for most businesses—including those dealing with large amounts of data streaming in and out such as video conferencing or virtual reality applications.

WiFi6 also brings increased range capabilities compared to earlier versions of Wi-Fi technology, which means fewer dead spots in your facility or office space due to weak signals from your router or access point (AP). With better coverage across larger spaces, you won't have as many issues with dropped connections or decreased performance due to distance from your APs—meaning more productivity and less downtime for your business operations overall.

To sum it up: if you're looking for better speed and performance from your wireless network without compromising coverage across larger areas in your facility, then you should seriously consider investing in the latest version of wireless tech: WiFi6! Not only is this tech capable of providing faster speeds with greater stability over longer distances; but it can also help decrease battery drain on mobile devices while increasing their overall lifespan too! Plus, with DanTech Services providing cutting-edge solutions that meet all these requirements (and more!), you can be sure that you'll be getting top-notch service no matter what kind of business operation you're running! So don't wait any longer – get ahead now by upgrading your existing network today! WiFi6 is now a standard addition to our Uplevel Systems deployments.

Enjoy the benefits of a modernized network without the capital expense!

Dan

Shiny New Gadget Of The Month:

Face Mask for Quiet Calls

The European Commission recently said passengers can use 5G on planes in Europe, even for midair phone calls. (That's not happening in the U.S.—yet.)

While it might make everyone else invest in noise-canceling headphones, more thoughtful talkers might look into Skyted.

Created by an Airbus alum and backed by the plane maker, this privacy mask uses aerospace materials and techniques to absorb 80% of voice vibrations.

This means you can place a phone call—or trash talk opponents in an online videogame—without bugging fellow passengers, office mates or domestic partners.

The high-tech mouth muffler, which starts at $400, is set to launch on Kickstarter in March.

Secure your Business: DanTech Services, Anchorage-Based Managed Services for Client-Focused Protection

As a business owner, you understand the importance of security and reliability when it comes to your systems. You want a partner who is knowledgeable, trustworthy and can provide comprehensive managed services that are customized to meet your needs. That's why business owners in Anchorage turn to DanTech Services.

DanTech Services is an Anchorage-based company that specializes in IT managed services. We understand the unique needs of our individual clients and strive to create the best possible solution that meets their specific requirements. Our team works closely with each client to develop their security strategy, maximize efficiency and minimize costs while providing top quality service.

At DanTech Services, we have a deep understanding of technology security from both a technical and strategic perspective. Our team has years of experience in cybersecurity and understands how important it is for businesses to remain secure online and protect their data from unauthorized access or malicious actors.

We offer comprehensive protection against cyber threats with several different managed service options including firewall installation, regular vulnerability scans, managed endpoint detection & response, SaaS application monitoring, as well as 24/7 monitoring & response services if needed.

DanTech Services offers full service solutions that are tailored specifically for businesses in Alaska which makes them an ideal partner for any business owner looking for reliable protection against cyber threats without breaking the bank on expensive IT solutions.

With our client-centric approach to cybersecurity, you can be sure that you're getting the best possible protection available at an affordable price point without sacrificing quality or performance. When it comes to keeping your business safe online, trust DanTech Services for all of your cybersecurity needs in Anchorage! Our operational expense model of managed services are reliable, secure, and cost effective so you can rest easy knowing your data is safe from any potential threats without breaking budget constraints!

Dan

Customer Testimonial:

I recently had the pleasure of working with Michael from DanTech Services and I could not be more pleased. Michael responded quickly to my text late at night when I was in a pinch, and his expertise was invaluable.

If you're looking for reliable service from professionals,
DanTech Services is your team!

They always go above and beyond to ensure their customers get the best possible experience!

Highly recommended!

Kristin Barquist
CFO
MyMed Supplies
Lux Infusion

Computer or Network Problems?

Call 907-885-0501

"Considering an app to manage your passwords?"
- continued from page 1

But customers often ignore best-practice instructions to choose unique and complex passwords for every account and instead fall back on familiar and simple passwords. Research repeatedly finds people admitting password reuse; in one small survey conducted in 2021, 24% of respondents reported that they reused an older password to secure their password-manager account.

Password manager services emphasize the importance of picking new and complicated master passwords, but they're not equally strict about it. Toubba's post, for example, mentions that LastPass did not require master passwords be at least 12 characters long until 2018, and outside researchers have found that LastPass used simpler techniques before then to generate encryption keys from these master passwords.

LastPass did not return two emails requesting comment.

If you recycled an older password for your LastPass account, you face the highest risk because that old password may have been leaked in a data breach, making it easy for attackers to try it on a copy of your data vault–an attack technique called "credential stuffing."

Your Email

"Just changing your LastPass password will not help here, as the old password will still be what's protecting the stolen password files," Sean Gallagher, principal threat researcher at Sophos, wrote in an email. He advised LastPass users to change passwords they'd saved in the service, as tedious as that may get.

Observing that "password cracking may not be necessary if the attackers can get the master key passwords by other means," Gallagher warned LastPass users to be wary of phishing emails purporting to be password-change requests from LastPass.

Is it worth paying for a password manager?

The case for password managers in general remains strong. For example, Apple and Google provide limited services for free, while third-party apps from Bit-warden (free and paid options available) and 1Password (paid only) consistently do well in independent reviews, offer better cross-platform compatibility, and don't require you to put so many digital eggs into one giant tech company's basket.

"Despite the LastPass breach, I still strongly recommend that people use password managers," emailed Lorrie Faith Cranor, director of Carnegie Mellon University's CyLab Security and Privacy Institute and a former chief technologist at the Federal Trade Commission.

As she told USA TODAY in 2021: "If you adopt a password manager, you don't have to think about coming up with unique and strong passwords anymore and you don't have to figure out how you are going to remember them."