

**DTS**

DanTech Services

Computers under control!™

Technology Times July 2024 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. “



Dan Foote
Owner/President

What's Inside:

Page 2

Are Mini PCs Worth Buying? Here's Everything You Must Know

Staying cyber-secure while traveling

Page 3

Fizz - an anonymous messaging app for harmless chatter among students: what could go wrong?

“Top cybersecurity trends for 2024?”
continued from page 1

Page 4

Shiny Gadget Of The Month:
RingConn Smart Ring
The Ultimate Wearable Device



Secure your future: Top cybersecurity trends for 2024

2023: cybersecurity trends in review

When we look back at 2023, we see that some predictions held true, whilst other trends took rather unexpected turns. Let us take a look at the most important predictions that materialized and the cybersecurity developments that surprised us.

Building towards a passwordless future

Most tech companies and consultants predicted an increased adoption of passwordless authentication. This trend largely played out as anticipated. Several major tech companies helped accelerate the passwordless future through high-profile implementations. Passwordless sign-in for commercial Azure Active Directory users and Apple's passkeys in iOS 16 and macOS Ventura are prime examples.

Consumer response has been largely positive, as passwordless systems remove the friction of memorizing credentials. We also saw an increased integration of passwordless authentication with zero-trust policies and identity and access management.

Ongoing supply chain problems

As unfortunately expected, supply chain attacks and vulnerabilities persisted in 2023. Several high-profile companies (BA, the BBC, Boots, Okta) fell victim to sophisticated supply chain attacks last year.

Expanding IoT attack surfaces

It wasn't a surprise that the proliferation of IoT devices would expand the organization's attack surface. Attackers consistently targeted vulnerable IoT devices to gain network access, leading to increased actions in IoT firmware updating, IoT monitoring, and network segmentation.

- Continued on page 3



Get More Free Tips, Tools, and Services at [https:// www.dantechservices.com](https://www.dantechservices.com)

Staying cyber-secure while traveling



Travel season is upon us, and while we appreciate the convenience of staying connected with our home or work during the journey, that also exposes us to many cyber security risks. One in five travelers is compromised while they're on the road. So how do you remain safe and guarded from cybercriminals?

Minimize the number of devices you take. The more gadgets you have, the greater your vulnerability. Even if your device isn't stolen, leaving it behind can cause added stress and inconvenience.

For those devices you decide to bring with you, secure them. Don't leave them unattended, like on a restaurant table while you're visiting the salad bar, or on a table at the pool while you're taking a dip to cool off. Additionally, set strong passwords or use biometric features on all your devices, including your laptop, tablet, and phone.

You should browse with caution. Be wary of free wifi networks, like those in hotels, which are often unsecure. To verify a site's security, look for the lock symbol in the address bar or an https at the beginning of the URL.

Avoid accessing sensitive information, such as banking sites or work sites, on public networks. Instead, use a Virtual Public Network, or VPN, which scrambles your data to make it unreadable to prying eyes.

Opt for mobile data connections rather than public Wi-Fi when browsing, or you can use your phone as a private hotspot for your other devices for secure browsing.

Enable the "find my phone" feature, which allows you to locate your phone, or remotely wipe data or disable the device if it falls into the wrong hands.

Staying cyber safe during your vacations is crucial to keep your personal information protected and help you maintain a peace of mind.

Are Mini PCs Worth Buying? Here's Everything You Must Know

In today's rapidly evolving technological landscape, do you often feel overwhelmed by the sheer number of new electronic products? When it comes to purchasing a new electronic device, do you find yourself struggling to make a decision? If you're an electronics enthusiast, a PC gamer, or a business professional who frequently travels, then the Mini PC we're introducing today might just meet all your needs. A Mini PC, also known as a microcomputer or a small form-factor PC, is a compact, mid-range, and budget-friendly computer device. It typically includes all the basic components of a computer, such as a processor, memory, and hard drive, but its size is significantly smaller than traditional desktops and laptops, making it portable and space-saving. Due to their small size and high cost-performance ratio, Mini PCs have been widely used in various fields such as homes, offices, and education. Many well-known computer brands, such as Apple, Dell, and Lenovo, have launched their own Mini PC products, further promoting the development of the Mini PC market.

What Are the Advantages of Mini PCs?

There are several reasons why Mini PCs are becoming increasingly popular:

Portability: Mini PCs are compact and lightweight, making them easy to carry around. This is especially convenient for business professionals and students.

Space-saving: Mini PCs take up significantly less space than traditional desktops and laptops. For space-constrained environments such as small apartments, offices, and student dorms, Mini PCs are an excellent choice.

Cost-effectiveness: While Mini PCs may not offer the same level of performance as high-end desktops and laptops, they are perfectly capable of handling the daily needs of most users, such as office work, browsing the web, and watching movies. Moreover, Mini PCs are typically priced lower than full-size desktops and laptops, making them a more cost-effective option.

Eco-friendliness: Due to their compact size, Mini PCs generally consume less power than traditional desktops and laptops, which aligns with modern environmental consciousness. Therefore, with the advancement of technology and the changing lifestyles of people, the various advantages of Mini PCs have greatly increased their popularity.

Who Should Buy a Mini PC?

Light Office Users: For light office tasks such as word processing and simple image editing, the performance requirements are not high. Regular large chassis take up a lot of office space, and laptops are not suitable for people who work in offices due to their small screens and poor keyboard feel. Therefore, in such scenarios, a Mini PC can save space while allowing users to easily take it to conference rooms for presentations or bring it home for work.

Users Who Need to Save Space: Mini PCs have a small footprint, which can effectively save your work or living space and make your office area look neater and more refined. Mini PCs will maximize their value in limited spaces.



- Continued on page 4

Fizz - an anonymous messaging app for harmless chatter among students: what could go wrong?



The Fizz app was created to allow students to post anonymously, intending Fizz to be a one-stop-shop for discussions on events, meeting classmates, commerce, and just a place to speak their mind. But as we all know, posts can get mean, especially when the poster remains anonymous.

Fizz opened to students at Vermont's largest High School in May. Within hours, havoc ensued -- posts escalating from jokes and memes to the public shaming of fellow students and accusations of affairs between faculty members or students.

It was originally called, "an uplifting digital space for Gen Z," by the two Stanford students who created the app. They wanted it to be a way for college students to feel less lonely and make meaningful connections on campus.

Posts rose in the feed based on students' votes, with the most harmful messages often springing to the top in short order. The "uplifting" chat app soon had high schoolers posting photographs of their classmates and mocking fashion choices or disabilities.

Students had to keep checking the app to ensure nothing damaging was posted about them. Some said they felt they just couldn't trust anyone. Fizz suspended its community at this high school after working directly with school administrators. "Our mission is to combat loneliness for Gen Z, and we have a zero-tolerance policy for bullying on Fizz," a spokesperson for the company said.

"Top cybersecurity trends for 2024?"

continued from page 1

Global harmonization of information, privacy and data regulation

Most tech followers expected a growing and globally carried momentum towards harmonizing privacy and data regulations across borders. Although some tentative steps towards this goal were taken, divergent national interests remained a crucial challenge to international information, privacy and data regulation. To this day, the European Union's GDPR is pretty much one of a kind and remains the most expansive data protection laws worldwide.

Unveiling the future: predicted cybersecurity trends for 2024

As 2023 draws to a close and we embark on 2024, the realm of cybersecurity is bound to experience some transformative changes. Time to take a look at the major cybersecurity trends and predictions for the coming year.

The growing presence of AI in security operations

In the slipstream of the success, growing popularity and democratization of generative AI (ChatGPT anyone?), AI and machine learning are expected to play a more critical role in cybersecurity operations from 2024 onwards. AI's ever-advancing data analysis capabilities are increasingly used for identifying and predicting cyber threats. ML algorithms are evolving to better recognize and respond to new threats, improving defensive measures over time.

These modern AI algorithms exceed human capacities in the field of threat data collection, threat detection and prevention. Many tech experts expect to see AI algorithms providing real-time threat analysis in 2024, enabling faster and more accurate responses to cyber incidents. ML will likely advance to adapt and update cybersecurity protocols autonomously. This removes the need for time-intensive and sometimes costly manual updates.

However, it's important to note that even as AI takes on a more prominent role, it can't exist without human intelligence. People will always be needed to oversee and guide these AI-driven systems. While AI algorithms excel in tasks like threat data collection and analysis, human experts provide the context and strategic decision-making that machines can't replicate.

We may even witness the emergence of AI-driven security bots in 2024. These smart digital actors are programmed to independently identify and neutralize cyber threats. The result? Network security becomes a more proactive affair, allowing you to detect and neutralize threats earlier than ever before. The growing importance of AI functionalities in the fast-evolving domain of cybersecurity signifies an important shift towards more intelligent and autonomous cybersecurity systems.

Outsourcing to managed solutions

Many companies already rely on external providers for sophisticated and specialized cybersecurity solutions. The reason? It's often very expensive and difficult to find the right experts and bind them to your organization in the long run. We predict that a growing number of organizations **are going to rely on managed services** to build and optimize robust and high-quality security solutions, ranging from a wide array of managed security services to advanced and modular cloud-based security platforms. Security-as-a-service (SECaaS) and similar solutions allow organizations in various industries to avoid overspending on security services that carry little benefit to their operations. It also gives them full access to knowledgeable security experts and the latest security tools for a fixed and manageable price.

With SECaaS in place, your IT team, chief information officer (CIO), and chief technology officer (CTO) can focus on meeting other organizational objectives.



RingConn Smart Ring The Ultimate Wearable Device

Experience more accurate biometric data with RingConn-lighter, refined, and personalized. Get tailored advice from continuous 24/7 monitoring for the perfect sleep and activity tracking experience.

- **High accuracy and sensitivity:** The finger's pulse signal is stronger and more accurate than the wrist, making it an ideal source of accurate heart rate data.
- **Fitness and Health Tracking:** Smart rings may also monitor your sleep patterns, heart rate, blood oxygen saturation, activity tracking, and stress index and provide insights into your overall well-being.
- **Personalization and Customization:** Smart rings often provide options for personalization, allowing you to choose different ring styles, colors, etc.

Compact and Stylish: Smart rings are generally small and lightweight, making them more discreet and comfortable to wear compared to larger wearable devices like smartwatches.

Please note that the ring can retain monitoring data offline for up to 7 days only. To ensure seamless data synchronization, it is advised to establish a Bluetooth connection between the ring and your phone within this 7-day window and synchronize the data to the app.

Users Who Need Portable Devices: The portability of Mini PCs makes them easier to carry around when moving, traveling, or working in multiple locations, without having to worry about weight and size.

Users Who Are Concerned About Cost-effectiveness: Compared to traditional hosts, Mini PCs have a higher cost-performance ratio. They can not only meet your budget needs but also ensure good product performance.

How to Choose the Right Mini PC Without Making Mistakes?

Choose Mini PC Specifications Based on Your Needs: Identify your purchasing needs, and then learn about and consult products based on those needs. This may help you choose the product you want more accurately. At the same time, the CPU specifications of a computer directly affect the system's operating efficiency and determine the scope of the computer's operation. For example:

For everyday office tasks, such as browsing the web and editing documents, you don't need a very powerful CPU. A low- to mid-range dual-core or quad-core CPU, such as Intel's i3 or i5 series or AMD's Ryzen 3 or Ryzen 5 series, should be sufficient.

Gaming and media creation: For gaming and media creation, you need a powerful CPU to handle graphics and video tasks. A high-end quad-core or more CPU, such as Intel's i7 or i9 series or AMD's Ryzen 7 or Ryzen 9 series, would be a better choice.

Choose the Mini PC You Want Based on Your Budget: Choose the product with the highest cost-performance ratio within your budget.

- 1. Budget of \$100-\$200:** Users in this price range can consider AMD's Ryzen 3 series or Intel's i3 series. These CPUs are suitable for light multitasking and media consumption.
- 2. Budget of \$200-\$300:** AMD's Ryzen 5 series and Intel's i5 series are ideal choices in this price range. These CPUs are suitable for moderate multitasking, light gaming, and media creation.
- 3. Budget of \$300-\$500:** In this price range, AMD's Ryzen 7 series and Intel's i7 series are excellent choices. These CPUs are suitable for heavy multitasking, high-end gaming, and professional-grade media creation.
- 4. Budget of \$500 and above:** For this price range, AMD's Ryzen 9 series and Intel's i9 series are the top choices. These CPUs are suitable for extreme multitasking, professional-grade gaming and media creation, scientific computing, and big data processing.

Please note that the above suggestions are mainly based on CPU price and performance. When making an actual choice, you also need to consider other factors, such as motherboard compatibility, power supply capacity, and heat dissipation performance.

Consider Brand and After-sales Service

When choosing a Mini PC or other electrical products, it is very important to consider the brand and after-sales service. Here are some specific suggestions:

Brand reputation: It is very important to choose a brand with a good reputation and credibility. A good brand will invest heavily in product quality, technological innovation, and user experience.

Warranty policy: A good warranty policy can ensure that you get a timely solution when there is a problem with the product.

Customer service: A good brand should be able to provide quality customer service, including pre-sales consultation and after-sales support.