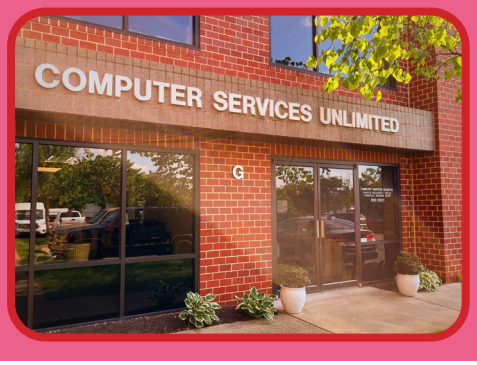


Connection

February 2025

We believe that experienced, reputable, and fast responding IT support should be the standard!

Our Services:

- Data Backup & Recovery
- Managed Services
- IT Consulting
- Network Security
- Cloud Computing
- Remote IT Services
- Cyber Security Training
- Mobile Device Management
- VoIP Phones

GOOGLE WILL START TRACKING DEVICES WITH FINGERPRINTS & SHARING DATA WITH ADVERTISERS

Google has announced a major change: starting February 16, 2025, companies using its advertising services can track users through "fingerprinting." This method goes beyond traditional cookies, offering deeper, cross-platform tracking across devices like smart TVs and gaming consoles. This new policy raises significant privacy concerns, especially since Google previously criticized fingerprinting as it can't be easily controlled or deleted by users.

(continued on page 2)

Let's get social!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

LinkedIn:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Newsletter:
www.csuinc.com/news

WHY THE CHANGE?

In its announcement, Google gave their answer for such fingerprinting - smart TVs, gaming consoles, and streaming services. "Internet users are embracing Connected TV (CTV) experiences, making it one of the fastest growing advertising channels. Businesses who advertise on CTV need the ability to connect with relevant audiences and understand the effectiveness of their campaigns."

It is cross-platform, cross-device ad tracking. Get ready for a steady stream of ads on your Smart TVs and gaming consoles in 2025.

WHAT IS FINGERPRINTING?

Fingerprinting collects data from your device, such as browser details or hardware information, to track you online—without relying on cookies. Unlike cookies, which can be deleted, fingerprints persist even after clearing your browsing data, allowing ongoing tracking without your consent. There are two types of fingerprinting:

Browser Fingerprinting: This gathers details about your web browser (e.g., Chrome, Firefox, Safari, Edge), such as browser type and version, screen resolution, time zone, language settings, and browser extensions/plugins.

Device Fingerprinting: Similar to browser fingerprinting, but deeper, it collects information from your device's hardware, including operating system type and version, processor details, memory and storage capacity, IP address, MAC address, network type, internet provider, and geolocation.

WHAT INFORMATION WILL GOOGLE COLLECT?

Starting in February 2025, Google will gather both browser and device fingerprints, then share that data with advertisers and third-party services. This change could make fingerprinting a replacement for third-party cookies, which users can usually control.

HOW FINGERPRINTING WORKS IN REAL LIFE

Fingerprinting can affect various aspects of your online experience. For example, search history could be sold to data brokers and used to influence insurance rates. Similarly, online stores may adjust pricing based on your perceived location, as detected through fingerprinting.

HOW TO PROTECT YOURSELF

While it's currently impossible to fully prevent fingerprinting, you can take steps to protect your privacy:

Use a VPN: A Virtual Private Network (VPN) hides your IP address, making it harder for data brokers to track your geolocation and associate it with your fingerprint.

Use a Private Browser: Browsers like Firefox, Brave, DuckDuckGo, or Tor offer

better privacy protection by blocking tracking and fingerprinting.

INCOGNITO MODE AND GOOGLE'S ROLE

Google's Incognito Mode does not protect against fingerprinting or tracking. While it prevents your browser from storing browsing history locally, it doesn't stop websites from collecting your data.

CONCLUSION

With this change, Google will provide advertisers with deeper insight into your online behavior, linking it to your real-life identity without your consent. In today's digital world, businesses and individuals must decide where they draw the line between convenience and privacy.

Tech Giggles!

Why did the computer breakup with the internet?

...

It found someone with a better connection!

Q&A

Q: Should everyone in my business use the same browser?

A: While it's not vital, it does make room for better consistency, support, and security. Whatever people use, make sure to check the security and privacy settings.

Q: My team doesn't have time to sit down for cyber security training together. Is it necessary?

A: Yes, training is critical for everyone. But it doesn't have to be classroom style. You can use interactive or online training that people can do when it suits them best.

Q: What's the best way to back up my data? And what should I backup?

A: The answer to this depends on your individual business needs. We can assess them for you and make recommendations – get in touch.

DeepSeek: What Is It? Is it Dangerous?

As you may have seen, DeepSeek, an AI app launched in 2023 by Liang Wenfeng, has been making headlines—especially after a January 2025 update. The app, which is similar to OpenAI and ChatGPT, utilizes reinforcement learning and boasts capabilities that have caught the attention of security experts.

What Is DeepSeek?

DeepSeek has quickly emerged as a strong competitor to U.S. tech giants like Meta, Google, and Microsoft. With its affordable price and high performance, it challenges the idea that cutting-edge AI requires billions of dollars in investment. DeepSeek's success is disrupting the tech sector, raising questions about the future of AI development.

Why We Do Not Recommend It

The risks associated with DeepSeek are primarily tied to its potential misuse.

- Privacy Concerns: DeepSeek collects sensitive user data, including keystroke patterns and device information, which raises privacy issues, especially as it can track and uniquely identify individuals.
- Risk of Chinese Government Access: As a Chinese company, DeepSeek may be subject to Chinese laws that could allow government access to user data for surveillance or geopolitical purposes.
- Potential for AI Misuse: DeepSeek's AI capabilities could be exploited for creating deepfakes, spreading misinformation, or fueling propaganda campaigns.

Why the Risks Are Greater with DeepSeek

Now you may think, "but similar problems and data collection methods are happening with other media platforms" but the thing is, DeepSeek's connection to a Chinese company heighten concerns about potential government access to this data. As a result, several US government

Instagram: computer_services_unlimited
Facebook: Computer Services Unlimited Inc.
Phone: (703) 968-2600

agencies, including the Navy, have prohibited their employees from using it.

Protect Yourself (if you use it...)

If you're considering using DeepSeek or are already using it, there are a few precautions you can take:

- Use a Separate Email: To reduce the amount of data shared with DeepSeek, register for the app using a new email account that is not tied to your other personal or business accounts. This will help ensure that the app cannot easily connect your DeepSeek interactions to other online activities.
- Avoid Using on Primary Devices: Experts suggest not using DeepSeek on your personal devices that contain sensitive information. If you must use the app, consider using an incognito or separate device that does not store your personal data.

Our Strong Recommendation: Just Avoid It

Given the significant privacy, security, and geopolitical risks associated with DeepSeek, we strongly advise against using it. The app's potential for surveillance and the misuse of AI makes it an unsafe choice, especially for those who prioritize their privacy. While some precautions might help reduce risks, the app's origins and the potential for government access to your data simply make it too risky to use in good conscience.

If you're looking for AI solutions that prioritize security and privacy, there are safer alternatives available, such as Copilot and ChatGPT. These platforms offer similar capabilities without the same level of risk.

Conclusion

DeepSeek may be an impressive piece of AI technology, but its data collection practices, its connection to the Chinese government, and the potential for misuse make it a risky choice for anyone who values their privacy and security. Overall, we recommend staying away from this app and choosing more trusted, secure options instead.

Gadget of the Month!

Orbitkey Hybrid Laptop Sleeve

$70.90 on Amazon!

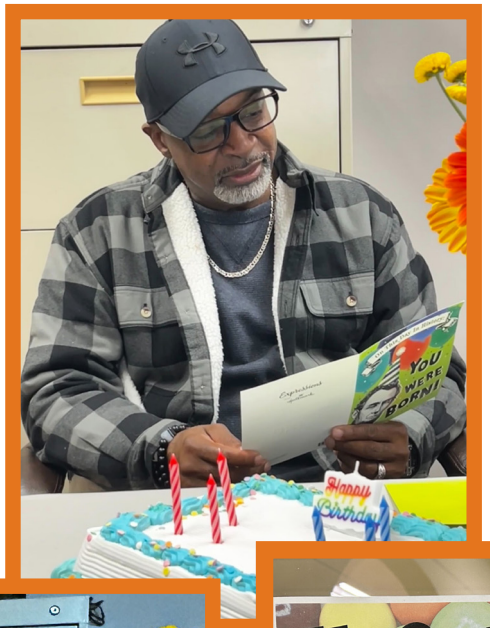
Orbitkey lets you transform any space into your workspace with its dual-function sleeve/desk mat. Made from vegan leather and recycled woven fabric, it combines functionality with eco-friendly materials.

It comes with a magnetic closure and a slim design that fits easily into any bag. The laptop pocket doubles as a mouse pad, making it a perfect on-the-go workspace. It's made for up to 14" or 16" laptops.

What's NEW at CSU?

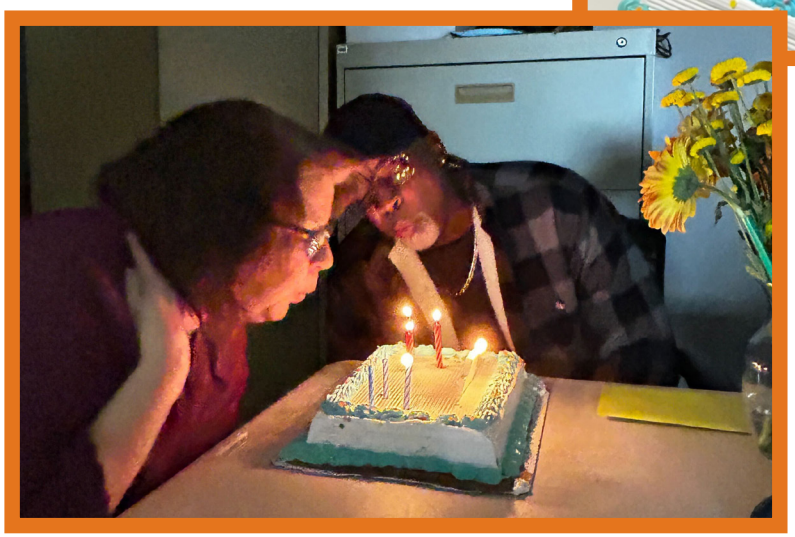
National Hat Day!

We rocked all kinds of hats that day! From bucket hats to cowboy hats, we were all lookin' good!



January Babies!

Michelle and Melvin (M&Ms) had their birthday celebrated with their favorite goodies and cake!



Instagram: computer_services_unlimited
Facebook: Computer Services Unlimited Inc.
Phone: (703) 968-2600

We have new 2025 family members! Please welcome...

Chisholm Law Group, LLC

PROGRESSION

EUROPEAN SPECIALISTS J&F Est. 1979

Chisholm Law Group is a referral from one of their employees– Thanks, Monica!
J & F Motors is a friendly business that specializes in luxury car maintenance!
Progression is a helpful staffing agency based in Reston!

We're thrilled to be partnering with these wonderful businesses!

Compliment Day brought extra positivity in the office! Everyone got a personalized compliment that brightened their day!

FEBRUARY BIRTHDAY!

Happy birthday to Bonnie! Our ready and helpful hand! Hope you have a sweet birthday!