



Connection

November 2024

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



Windows 10 End of Life (EOL)

EOL Date: Windows 10 support will end on October 14, 2025, a decade after its launch.

Impact of EOL:

- No more technical support or security updates, this leaves Windows 10 systems vulnerable to threats.
- Final Windows 10 version, 22H2, will receive monthly security updates up *until* EOL.

Reasons for Transition:

Although your Windows 10 PC will continue to function after reaching the end of support, it will be increasingly vulnerable to security risks, including viruses, malware, and cyber threats. Without monthly security updates, any newly identified vulnerabilities will go unpatched, leaving your system less secure.

(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



For individuals and businesses, this could lead to potential data loss, cyberattacks, or declining system performance over time. Understanding the implications of Windows 10's EOL is essential for safeguarding your devices and data.

Upgrade Options:

1. **Upgrade to Windows 11:** Recommended for compatible systems; includes enhanced features and security.
2. **Continue Using Windows 10:** Possible but risky; no security updates will be available.
3. **Purchase a New Device:** Ideal for older PCs that cannot upgrade to Windows 11.

Windows 11 Versions Support:

- Windows 11 Home and Pro will have at least 5 years of mainstream support, followed by 5 years of extended support.
- Business-focused editions also offer similar support lifecycles with added features.

Preparation Steps:

- **Back Up Files:** Ensure data safety by backing up important files.
- **Check Compatibility:** For CSU contract clients, we will run reports on your equipment and set up a meeting with you to discuss our findings. If you're not a contract client, please call to make an appointment for us to evaluate your systems.
- **Consider Hardware Updates:** New devices ensure compatibility with Windows 11.

Security Post-EOL:

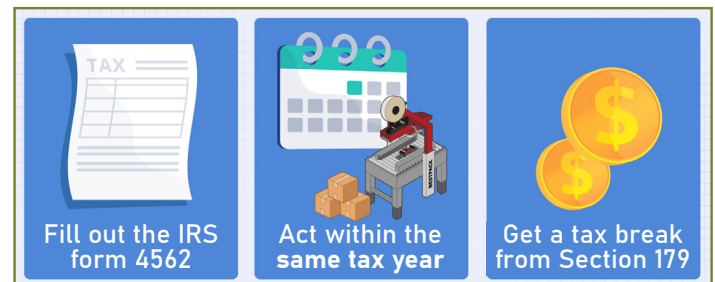
- Microsoft MAY offer an extended support program (they have in the past). This would only be for critical updates. There is no guarantee they will offer this option

Now is the time to plan for the Windows transition! Contact us if you would like help navigating the transition from Windows 10 to Windows 11.



Understanding Section 179 Deductions and How They Can Benefit Your Business

Section 179 is a federal tax deduction that allows businesses to deduct the total cost of new equipment in the year it is placed into service—including computers. This means if you need a new computer altogether for this upgrade, get it now so you can have it as a deduction on your 2024 taxes!



Go to our website blog to learn more:
<https://www.csuinc.com/2024/10/24/understanding-section-179-deductions-and-how-they-can-benefit-your-business/>



8 TIPS FOR SAFEGUARDING YOUR GADGETS WHILE TRAVELING OVER THANKSGIVING

Traveling with technology has become a necessity. Whether for work, communication, or entertainment, we rely heavily on our devices. But traveling exposes these gadgets to various risks. Theft, damage, and loss are common concerns:

- 1. Use Protective Cases:** A high-quality protective case can help prevent damage from drops, bumps, or spills, while screen protectors can safeguard against scratches and cracks.
- 2. Leverage Tracking Apps:** For iPhones, use "Find My iPhone," and for Android devices, use "Find My Device." These apps can help you locate your device if it gets lost or stolen.
- 3. Keep Devices Close:** Keep them in a secure bag or backpack with anti-theft features, and avoid leaving them unattended in public spaces.

4. Use Strong Passwords: Protect your devices with strong, unique passwords. Enable biometric authentication (like facial recognition) for an extra layer of security.

5. Be Cautious with Public Wi-Fi: Public Wi-Fi networks can be targeted by hackers. Avoid accessing sensitive information, like bank accounts, on public networks. If you need to use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your internet connection.

6. Back Up Your Data: Regularly back up your data to the cloud or an external hard drive. This ensures that, in case of loss or theft, you won't lose important files, photos, or contacts.

7. Be Mindful of Your Surroundings: Stay aware of your surroundings, especially in crowded or unfamiliar places. Avoid displaying your devices in situations where they could attract unwanted attention. Be cautious when someone gets too close or tries to distract you, as it may be a diversion for theft.

8. Use Anti-Theft Accessories: Consider investing in anti-theft accessories, such as lockable bags, cable locks for laptops, or anti-theft backpacks. These accessories can deter thieves and make it more challenging for someone to steal your belongings.

By following these best practices, you can significantly reduce the risk of mishaps with your devices while traveling, allowing you to focus on enjoying your trip!

Gadget of the Month!

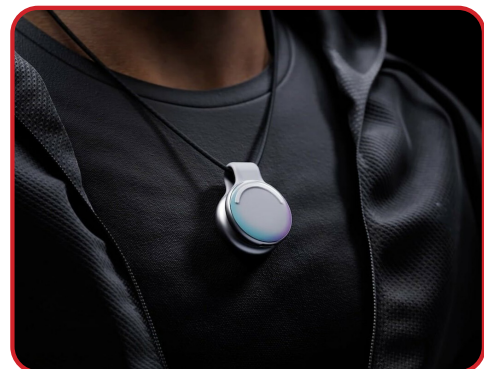
Limitless AI Pendant

A lightweight personalized AI wearable that is weatherproof and Wi-Fi/Bluetooth enabled.

It is usable on any device including the web, your phone, a Mac, or PC.

Pendant works with any meeting tool, has unlimited storage, and offers data encryption.

It remembers what you say throughout the day, from meetings or impromptu conversations.



**Preorder for \$99 on
Limitless.ai!**



7 Common Scams During Black Friday and Cyber Monday and How to Avoid Them

As Black Friday and Cyber Monday approach, shoppers seek great deals, but scammers are also on the prowl. Here are 7 common scams to watch out for, plus tips to protect yourself.

1. Fake Coupons

Scammers often circulate fake coupons that promise incredible discounts. These fraudulent offers are typically shared via email, social media, or deceptive websites that closely resemble those of legitimate retailers.

How to Avoid: Always verify coupons by checking the retailer's official website or app. Be cautious of clicking links in unsolicited emails or messages.

2. Phony Websites

Fraudulent websites may impersonate real online stores, using similar logos, branding, and slightly altered URLs to deceive shoppers into providing personal information.

How to Avoid: Look for secure website

indicators, such as HTTPS and a padlock icon in the address bar. Before making any purchases, read reviews and conduct a quick search to confirm the site's legitimacy. Be vigilant for unusual characters or misspellings in the URL.

3. Fake Delivery and Non-Delivery Scams

Scammers may send fake delivery notifications or claim that a package cannot be delivered, attempting to lure you into providing personal information.

How to Avoid: Track your orders directly through the retailer's website or app. Avoid clicking on links in suspicious messages and be wary of unsolicited delivery notifications.

4. Fake "Order Issue" Scams

You may receive emails claiming there's a problem with your order and requesting personal details. These emails often appear to come from well-known retailers.

How to Avoid: Always contact customer service directly using official channels to verify any issues. Avoid providing personal information through links in unsolicited messages.

5. Account Verification Scams

Scammers may send emails or texts requesting that you verify your account information, often including links to fake login pages.

How to Avoid: Never provide personal information through links in unsolicited messages. Instead, log in directly to your account via the retailer's official website.

6. Gift Card Scams

Fraudsters may offer discounted gift cards or ask for payment via gift cards. Once you provide the card numbers, the scammer can quickly deplete the balance, leaving you with a worthless card.

How to Avoid: Always purchase gift cards from reputable retailers and never use them to pay unknown individuals.

7. Limited-Time Offers

Be cautious of deals that seem too good to be true, especially if they pressure you to act quickly. These especially appear on social media.

How to Avoid: Research prices and compare them to ensure you're getting a legitimate deal.

Stay Safe While Shopping

Nothing ruins holiday shopping like finding fraudulent charges on your credit card or receiving gifts from untrustworthy sources. Cybercriminals take advantage of eager shoppers during the holiday rush. By verifying sources, checking website security, and avoiding unsolicited links, you can ensure a safer and more enjoyable shopping experience this season!

Tech Giggles!

Why did the
computer go to
the dentist?

To get his
Bluetooth
checked!



NOVEMBER ANNIVERSARIES

Majority of our team has their anniversaries this month! Can't do it without them.

Cheers to many more years!



Will has been with CSU for 4 years as a Network Engineer. Although he's 4,264 miles away, he still works hard and keeps the CSU fam updated with the Alaskan beauty he explores!



Byron has been with CSU for 1 year as a Network Engineer. We love the excellent way he fills out tickets and we appreciate his patience, laugh, and the chill vibes he brings to work!



Paola (Pow-ola) has been with CSU for 1 year as a dispatcher. We greatly appreciate her role and customer service that creates a smooth transition to getting tech issues solved!



Bonnie has been with CSU for 9 years as a on-call Administrative Assistant. So glad she cares so much and is willing to come out of retirement to help whenever we need her!

What's NEW at CSU?



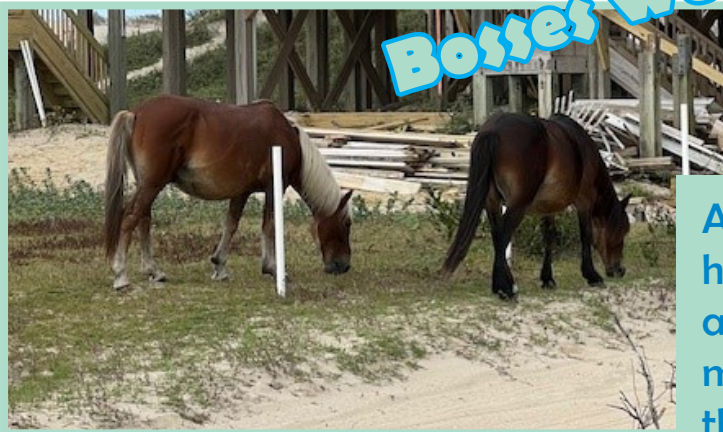
Hero Day! Caitlyn as Superman, Mike as Mr. Incredible, Melvin as Batman, Chuck as Trash...man?, Byron had the inspirational Deadpool, and Michelle with the ultimate hero, can you guess who was on her shirt?



On October 1st it was National Homemade Cookies Day! Obviously, Caitlyn had to bring in yummy homemade cookies to start the month off right!



Bosses Went To The Beach!



As expected, Michelle forgot to take pictures of her and the fam. But also as expected, she got all the animal pictures including horses... and more horses. She highly recommends going to the beach on off season - so peaceful!

NOVEMBER BIRTHDAY!

Happy Birthday to the bald and beautiful Will who makes the world a little brighter with his humor! May your day be filled with laughter, warmth (just kidding, keep it chilly for Mr Alaska!), and all the joy you bring to others. Here's to another year of adventures in the cold! Enjoy your special day, Will!



Treat 'em Like Royalty: National Boss's Day

Dearest Reader,
On Boss's Day, we treated our bosses with the highest regards in crowning them as king and queen of CSU. But we know who the true ruler is...



Pumpkin Carving Competition!

We posted the pumpkin contestants on our Facebook page. You all voted and the winner is... Alyssa!



Dressing up for Halloween!



Clown 1, Daphne, Shaggy, Track Suit Mike, Clown 2, Hobbit, Scooby-Doo, Plague Doctor, and Dr. Cloud