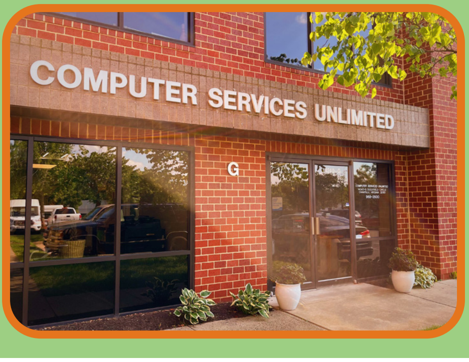


Connection

March 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

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

Spring Cleaning for Your Digital Life: The Importance of Cyber Hygiene

Spring is the perfect time to refresh more than just your home—your digital life needs attention too! Just like organizing your space, maintaining your tech ensures you stay secure and efficient all year long.

Cyber hygiene involves everyday practices that protect your devices, data, and online activity from threats like ransomware, phishing, and identity theft. Think of it as the digital equivalent of washing your hands: simple but essential for safety.

(continued on page 2)

Good cyber hygiene includes regular updates, strong passwords, and avoiding risky online behavior to prevent digital disasters.

Here are some essential cyber hygiene practices you can adopt this spring to clean up your digital life and improve your online security:

1. Change Your Passwords Regularly

Passwords are your first line of defense against unauthorized access to your accounts and devices. However, with so many online accounts to manage, it can be tempting to reuse passwords or choose weak ones. A quick spring cleaning for your passwords can make a big difference.

- Use Strong, Unique Passwords: Avoid easily guessed information and create complex passwords with a mix of letters, numbers, and symbols.
- Use a Password Manager: A password manager stores and generates secure passwords for you.
- Change Passwords Regularly: Update critical passwords (like banking or email) every few months to minimize the risk of compromise.

2. Keep Software and Devices Up to Date

Whether it's your operating system, apps, or antivirus software, keeping everything updated is one of the simplest yet most effective ways to protect yourself from cyber threats.

- Enable Automatic Updates: Set software to update automatically so you don't have to worry about it.
- Patch Vulnerabilities: Regular updates fix security issues that hackers may exploit.
- Upgrade Hardware When Needed: If your devices no longer receive updates or support, it's time for an upgrade.

Note: If you haven't already, upgrading to Windows 11 is important. Reach out and we'll get it set up for you!

3. Be Cautious of Suspicious Links and Emails

Cybercriminals love to trick people into clicking on malicious links or downloading harmful attachments. This is often how phishing attacks, malware, and ransomware are spread.

- Don't Click Unknown Links: Avoid clicking links or attachments in emails from unfamiliar sources or unusual messages from known contacts.
- Verify Email Addresses: Check the sender's email address carefully to spot phishing attempts.
- Watch for Red Flags: Be cautious of poor grammar, urgent language, or requests for personal info—common signs of phishing.

4. Secure Your Wi-Fi and Devices

Your Wi-Fi network and devices are gateways to your personal information, so make sure they're properly secured.

- Change Default Router Passwords: Routers often come with default passwords that are easy to guess. Set a strong, unique password for your router to prevent unauthorized access.
- Use Encryption: Ensure your Wi-Fi is

encrypted using WPA3 (or WPA2, at a minimum). This prevents outsiders from snooping on your internet traffic.

- Enable Device Encryption: Many devices, including smartphones and computers, offer encryption features that protect your data in case the device is lost or stolen.

5. Backup Your Data Regularly

No one wants to imagine losing important documents, photos, or business files. One of the best ways to protect yourself from data loss due to cyberattacks or hardware failure is by backing up your data regularly.

- Use Cloud Backup Services: Cloud-based services like Google Drive, iCloud, or Dropbox automatically back up your files to a secure server. Make sure your backup is up to date.
- External Hard Drives: For added protection, use external hard drives to create offline backups of critical data

Conclusion

This spring, give your digital life a refresh by practicing good cyber hygiene—change passwords, update software, be cautious of suspicious links, secure devices, and back up data. These simple steps will reduce the risk of cyberattacks and improve security.

Cyber hygiene is an ongoing commitment, and with CSU's support, we handle these tasks for you—updating passwords, software, providing cybersecurity training, and backing up your data. If you'd like coverage for your personal devices, just reach out!

Happy spring cleaning!

Tech Giggles!

Why don't leprechauns ever go online?

...

Because they don't want anyone hacking into their gold!

HOW PASSWORD MANAGERS PROTECT YOUR ACCOUNTS

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

You only need to remember one password, the master password. This master password lets you access all your other passwords.

Types of Password Managers

- A local desktop manager for your device
- Browser-based password managers integrated within your web browser
- Cloud-based password managers accessible from any device with an internet connection

Why Use a Password Manager?

It Helps You Create Strong Passwords:
Password managers generate long, random passwords that are hard to crack.

It Remembers Your Passwords:
With a password manager, you don't need to memorize many passwords. The tool does this for you.

It Keeps Your Passwords Safe:
Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

Password Generation:
Good password managers can create tough, unique passwords for you.

Auto-Fill:
Many password managers can fill in your login information on websites. This saves time and avoids typos.

Secure Notes:
Some password managers let you store credit card numbers or important documents.

Password Sharing:
Some tools let you share passwords safely with family or coworkers.

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Make sure it works on all your devices.
- Research the features you want and the price you can afford.

Top 8 Password Managers

- **1Password**
- **LastPass**
- **Dashlane**
- **Bitwarden**
- **Keeper**
- **NordPass**
- **Zoho Vault**
- **Enpass**

Consider using a password manager today to improve your online security. If you need help choosing or setting up a password manager, contact us today.

7 WAYS USING AI FOR WORK CAN GET COMPLICATED

AI is going to change how we work. It can make some tasks easier. But it can also cause problems. Let's look at some ways AI can make work tricky.
Where can AI go wrong?

1. **Incorrect Information:** It may mix up facts or use data that is too old.
2. **Weird outputs:** It may write utter nonsense or create odd images.
3. **Biases:** AI can be biased since it learns from data given to it by humans.
4. **Job Loss:** Some people fear that AI will steal their jobs.
5. **New skills needed:** AI also needs workers to acquire new skills.
6. **Teamwork:** The use of AI can affect teamwork between humans.
7. **Privacy:** AI requires a lot of data to operate, which causes privacy concerns.

AI can be helpful at work, but it's not perfect. We have to use it with care. If you have questions about using AI at your job, contact us today. We can help you use AI in a smart and safe way.

Gadget of the Month!

$149 on Amazon

Timekettle Translator Earbuds

Timekettle translator earbuds provide real-time translation between languages. The earbuds connect to a smartphone app, which acts as the translator.

When 2 people speak in different languages, the earbuds capture the audio and send it to the app for processing. The app then translates the speech and delivers the translation directly to the user's earbuds.

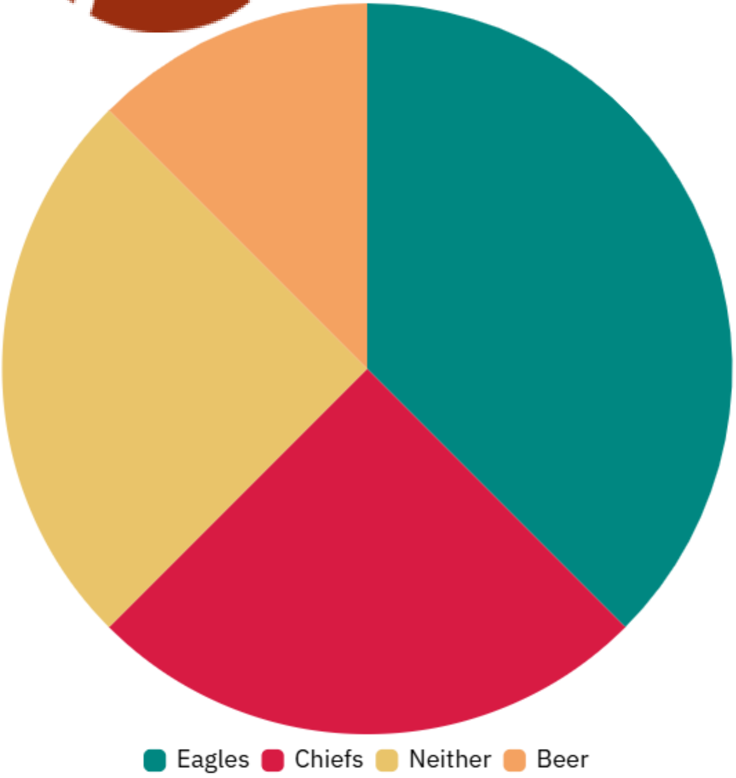
The system supports multiple languages and is designed to provide seamless communication in conversations, making it ideal for travelers or business interactions across language barriers.

What's NEW at CSU?

Superbowl!

None of the CSU family had their team in the superbowl, so the following day we flaunted our favorite sports teams!

But even though none of us had our team in the game, we still had a team we cheered for. Michelle and Chuck were cheering for the Chiefs, while Caitlyn, Melvin, and Paola were rooting for the winning team... the Eagles!

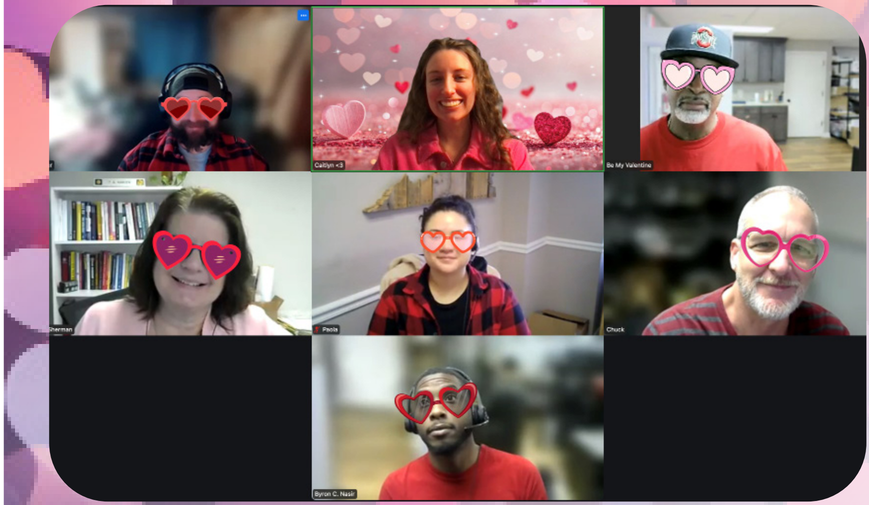


March Birthdays!

Happy birthday to Byron and Luis! They are not only alike in their birth months, but they are both very humorous and hard working! Wishing you two nothing but love and luck this year!

You all put in your suggestions on our Facebook and Instagram... and the best name for our beast of a printer is *drum roll* Bob Marley!

Be My Valentine?



For valentines day, the CSU family wore pink and red to celebrate. But... Caitlyn used photoshop to enhance the festivites! So, of course everyone received some heart glasses!

Do you know any businesses in need of I.T.? It could be one where a family member or friend works, or one down the road from your business. Send them our way! We *blossom* with referrals and would be happy to help :)