CSU Connection OCTOBER 2023

You take care of running your business, we'll take care of your technology.

Cybersecurity Skeletons in Your Business' Closet...

Let's dive into a topic that might give you the chills—**cybersecurity skeletons in the closet.** You may not have old skeletons hidden away in the basement, but there's a good chance of cybersecurity vulnerabilities lurking in the shadows... just waiting to wreak havoc.

You can't fix what you can't see.
It's time to shine a light on these hidden dangers, so you can take action to protect your business from potential cyber threats.

Outdated Software: The Cobweb-Covered Nightmare

Running outdated software is like inviting hackers to your virtual Halloween party.

When software vendors release updates, they often include crucial security patches. These patches fix vulnerabilities that hackers can exploit. Keep everything up to date to ensure your digital fortress is secure.

Weak Passwords: The Skeleton Key for Cybercriminals

If your passwords are weak, you might as well be handing out your office keys to cybercriminals. Instead, create strong and unique passwords for all accounts and devices. Consider using a mix of upper and lowercase letters, numbers, and special characters.

Unsecured Wi-Fi: The Ghostly Gateway

Ensure your Wi-Fi is password-protected. Make sure your router uses WPA2 or WPA3 encryption for an added layer of security. For critical business tasks consider a virtual private network (VPN). It can shield your data from prying eyes.

Lack of Employee Training: The Haunting Ignorance

Employee error is the cause of approximately 88% of all data breaches.

Without proper cybersecurity training, your staff might **unknowingly fall victim** to phishing scams. Or inadvertently expose sensitive information.

Regularly educate your team about cybersecurity best practices such as:
-Recognizing phishing emails
-Avoiding suspicious websites
-Using secure file-sharing methods

No Data Backups: The Cryptic Catastrophe

Imagine waking up to find your business's data gone, vanished into the digital abyss. Without backups, this nightmare can become a reality.

Embrace the 3-2-1 rule. Have at least three copies of your data, stored on two different media types. With one copy stored securely offsite.

No Multi-Factor Authentication (MFA): The Ghoulish Gamble

Adding MFA provides an extra layer of protection. It requires users to provide extra authentication factors. Such as a one-time code or passkey. This makes it much harder for cyber attackers to breach your accounts.

Disregarding Mobile Security: The Haunted Phones

Ensure that all company-issued devices have passcodes or biometric locks enabled. Consider implementing mobile device management (MDM) solutions.

These will enable you to enforce security policies.

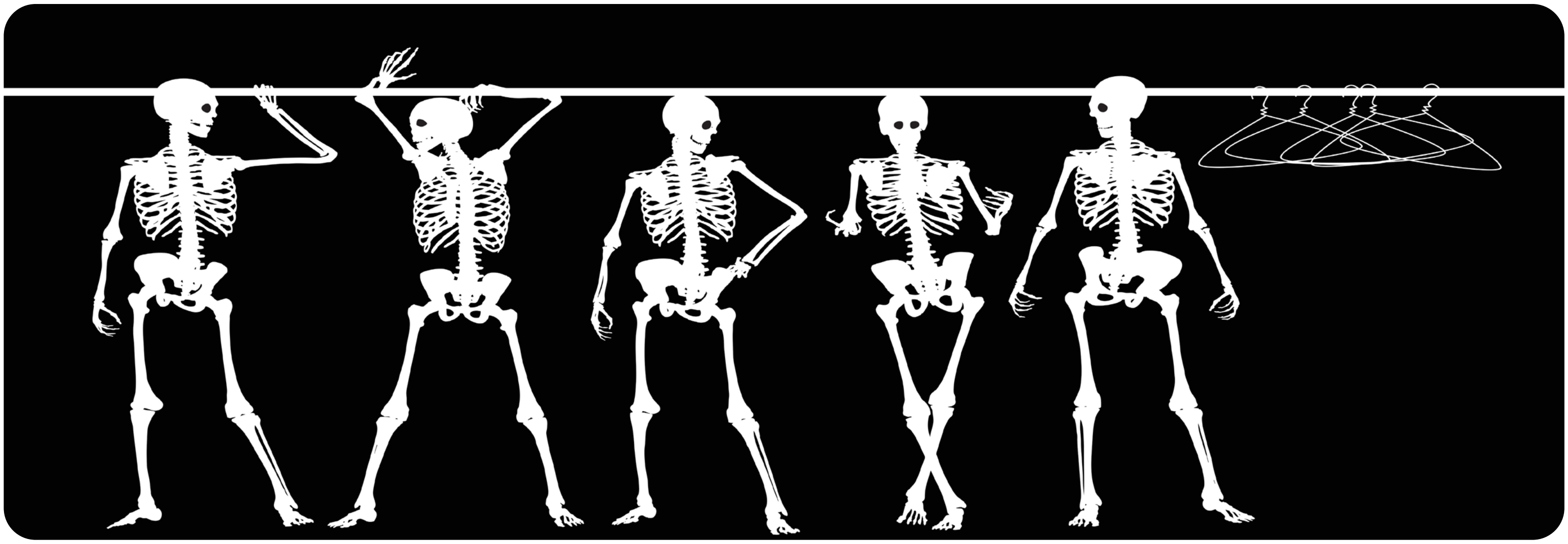
Shadow IT: The Spooky Surprise

Shadow IT refers to the use of unauthorized applications within your business. It might seem harmless when employees use convenient tools they find online.

Regularly audit your systems to uncover any shadow IT lurking under cover.

Incident Response Plan: The Horror Unleashed

Develop a comprehensive incident response plan. It should outline key items such as how your team will detect, respond to, and recover from security incidents. Regularly test and update the plan to ensure its effectiveness.



9 REASONS TO USE AIRPLANE MODE EVEN IF YOU'RE NOT TRAVELING

Most people are familiar with their device's Airplane Mode. You've probably used it when jetting off to exotic locations. But did you know that it's not just for globetrotters?

That's right! **Airplane Mode isn't only for flying; it can be a handy feature for your everyday life.**

Here are some top reasons why you should consider toggling it on, even if you're not traveling.

1. Save that precious battery life

2. Boost your charging speed (by about 4x)

3. A tranquil escape from notifications

4. Focus Mode: Engaged!

5. Prevent embarrassing moments

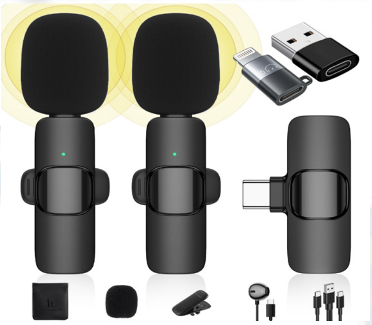
6. Roaming woes, be gone!

7. A digital detox

8. Avoid unwanted radiation

9. Save data and money

Gadget of the Month:



Aisizon Wireless Clip Mic

The Aisizon Wireless Clip Mic is a versatile and high-quality microphone that allows you to capture clear and professional audio wirelessly.

With its compact design and easy-to-use clip, it can be conveniently attached to your clothing or any other surface, providing hands-free recording for various applications such as interviews, presentations, vlogging, and more.

This is the perfect companion for capturing crystal-clear audio on the go.

Get yours today at **https://www.amazon.com/Microphones-Microphone-Aisizon-Smartphone-Recording/dp/B09JNLWYSN**

BOO! DON'T BE TOO FRIGHTENED BY THESE SCARY AND DISTRUBING CYBERSECURITY STATISTICS...

- It takes an average of **315 days** to detect and contain data breaches caused by a cyberattack.
- The average cost of a data breach has risen to **$3.86 million** with the average lost business in the aftermath of a cyberattack at ***$1.52 million.***
- The average **ransomware fee** demanded has risen to $***170,000.***
- **85%** of cybersecurity breaches are caused by **human error.**
- **64% of Americans** admit not knowing what steps to take after being notified of a data breach.

Get More Free Tips, Tools and Services At Our Website www.csuinc.com

How To Stay Safe on Social Media: A Series

Part 6: SnapChat

Snapchat is a private messaging app where short-lived content is shared, so it may seem like an unsuspecting platform for hackers. You might be curious as to why someone would hack Snapchat. The main motives could be **illegally spying, blackmailing, or obtaining private information like your phone number, passwords, etc.**

How To Tell A Fake Snapchat Account From a Real One:

- Check their Snap score. This will show if they're actively using the platform. If they claim to be an influencer and have a Snap score of just a few hundred, it's likely a scam.
- Look at the Snap map. Does their real-life location match what they say in their profile?
- Search their profile/story photos in Google image search. Scammers will steal images from other sites and use them for their fake accounts. Upload a photo to Google image search to see where it came from.
- Check if they have a Bitmoji. A Bitmoji is the cartoon avatar by a person's name. Because it's so common for Snapchat users to have these, it can be a red flag if an account isn't using one.
- Think about what they're asking you. If a random account adds you and starts asking for "help" or sending you strange links, you should probably block them. This also goes for your friends. If someone you know starts sending you strange messages, contact them on a different platform and ask if everything's OK.

Fake accounts often feature attractive models and people flaunting cash, luxury goods, and sports cars. **But never forget the golden rule of fraud prevention:**

"If it seems too good to be true, it probably is."

Snapchat (continued)

How To Prevent Snapchat Scams:

• Be suspicious of all links and QR codes in messages, even if they come from your friends (whose accounts may be hacked) or a lookalike Snapchat email. For added security, consider using antivirus software. This will automatically block malware and other malicious viruses for you.
• Never add strangers to your Friends List or accept unknown friend requests, even if they claim to be someone you might know.
• Text, email, or call your friends if you see sketchy behavior. Let them know their account may have been hacked.
• Never share your login credentials or trust threatening messages claiming to come from Snapchat. Snapchat will never leak your images or ask for your password or My Eyes Only passcode.
• Always create a strong password to prevent scammers from hacking into your account. Use a unique, hard-to-guess combination of at least 10 upper and lowercase letters, numbers, and symbols. Don't reuse this password for anything else. To help you keep track of these long passwords, consider a password manager.
•Set up Two-Factor Authentication (2FA) - but not SMS. 2FA makes your Snapchat more secure by sending a unique code to your device anytime you log in. However, hackers can bypass SMS authentication if they get access to your phone. Instead, use an authenticator app like Okta or Google.
•Adjust your privacy settings. Limit who can send you Snaps, view your Stories, see you in Quick Add, and find your location on Snap Map. Consider turning on Ghost Mode, so no one can see where you are.
•Keep your email and phone number associated with your account updated. This will help verify that your account belongs to you if you ever lose access to it.
These security tips ensure you and your teen can still have fun on Snapchat without putting their identity or your financial information at risk.

Sources and additional information:
•Anyone Can Hack Your Snapchat—Here's How to Stop Them
(https://www.makeuseof.com/how-to-hack-snapchat/)
•Snapchat Scams: Don't Fall for These 7 Insidious Scams
(https://www.aura.com/learn/snapchat-scams)

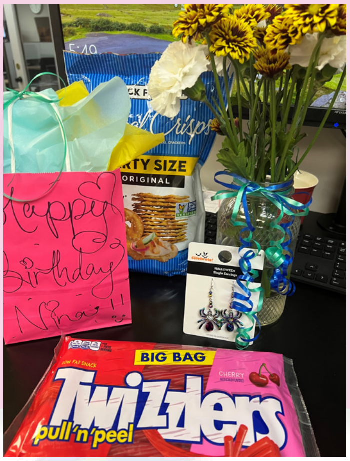
What's Up With The CSU Team?

Lots of Celebratin'!

When you're at CSU, celebrations are no small thing.

Happy Birthday to Ms. Nina!

We appreciate all your hard work and excellent attention to detail. You are one special gal!



Happy 1 Year Anniverary to Our Dependable, Go-to-Guy, Right-Hand-Man, Heath!

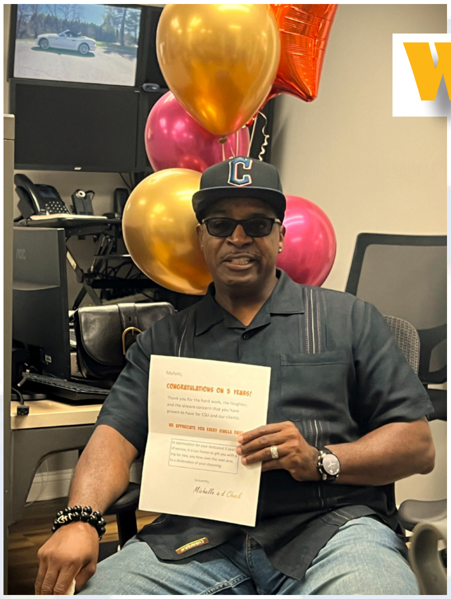
We can always count on you. Thank you for your dedication to CSU, and cheers to many more memories to be made!

Happy Birthday to our very own, one-of-a-kind, irreplacebale, Wanda!!

You are an incredible and valuable asset to our team. Thank you for your hardwork and genuine compassion for our us, animals, and clients!

Happy 5 Year Anniversary to our TALENTED, LOYAL, AND SUPER SMART friend and employee, Sir. Melvin!

Acknowledging his stellar work for the past 'half-decade', CSU has gifted Melvin and his wife a special trip to a destination of their choice! Where will they go.....
Stay tuned!



Melvin,

CONGRATULATIONS ON 5 YEARS!

Thank you for the hard work, the laughter, and the sincere concern that you have proven to have for CSU and our clients.

WE APPRECIATE YOU EVERY SINGLE DAY!

In appreciation for your dedicated 5 years of service, it is our honor to gift you with a trip for two, any time over the next year, to a destination of your choosing.

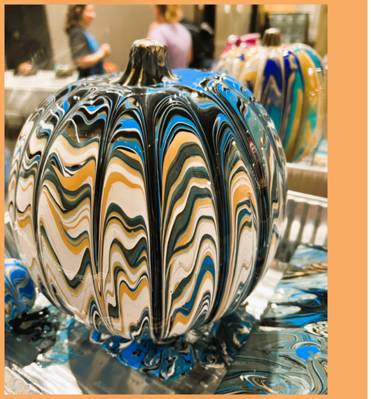
Sincerely,

Michelle and Chuck

WELCOME FALL!

We are staying creative around here-
Welcoming the new season with
Michelle's newfound hobby,
paint pouring!

What better object to have fun with than a nice, plump pumpkin?!



What's a creative craft you'd like to try this season?
Get out and go do it!

Stay connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Version of Newsletter:
www.csuinc.com/news

Our Services:

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

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

CSU COMPUTER SERVICES UNLIMITED

Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity, and profitability.

Proudly serving our community for over 30 years
COMPUTER SERVICES UNLIMITED

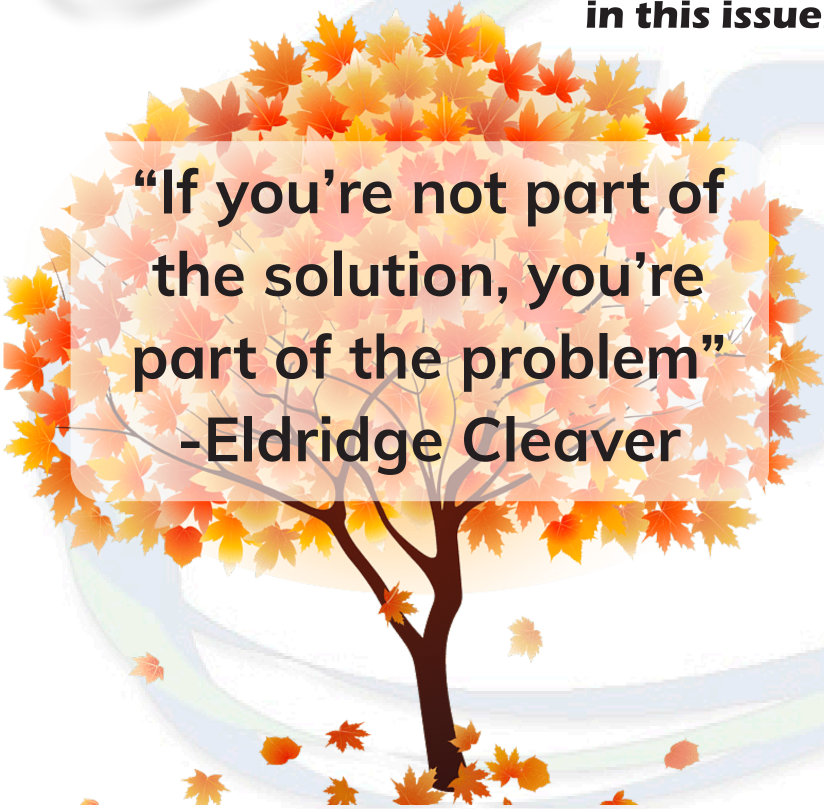
Computer Services Unlimited
14240-G Sullyfield Cir.
Chantilly, VA
www.csuinc.com

Connection

OCTOBER 2023

You take care of running your business, we'll take care of your technology.

in this issue...



"If you're not part of the solution, you're part of the problem"
-Eldridge Cleaver