Connection

August 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

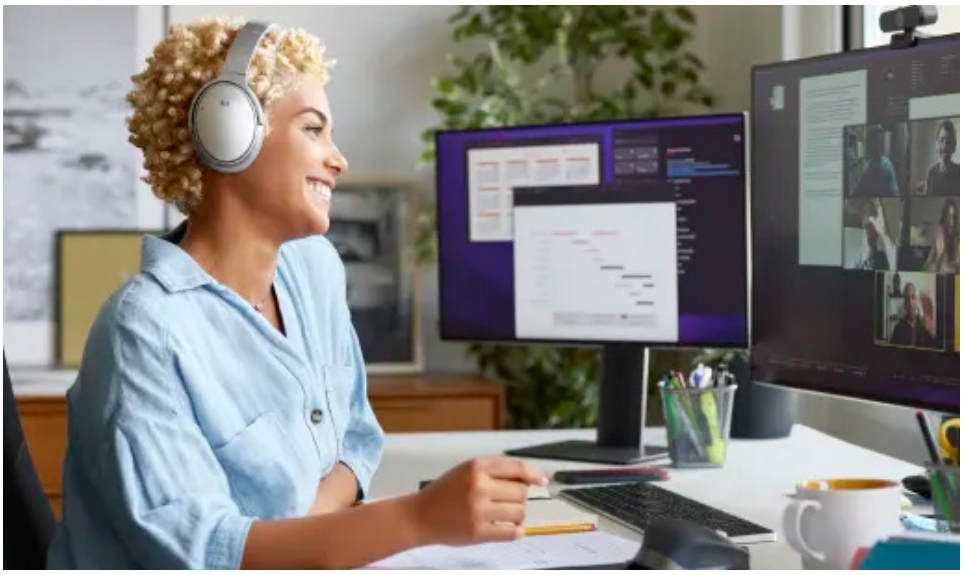
Let's get social!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Newsletter:
www.csuinc.com/news



TECH-SAVVY WORKSPACES:

HOW TECHNOLOGY DRIVES OFFICE PRODUCTIVITY

Gone are the days of paper-laden desks and rows of filing cabinets. The modern office is a hub of innovation. Technology plays a starring role in this transformation. The right tech tools can significantly boost your team's productivity. Including streamlining workflows and fostering collaboration. Is your company leveraging technology as well as it could? This article dives into the ways technology fuels office productivity. We'll explore the benefits and provide tips for creating a tech-savvy workspace.

Boosting Efficiency:
Technology as a Time-Saving Ally

The core benefit of technology in the office is its ability to save valuable time. Here are some key ways tech streamline workflows free up your team to focus on high-value tasks.

Automation Powerhouse

Repetitive tasks can be automated, eliminating manual effort and reducing errors. Imagine expense reports auto-populating. As well as scheduling meetings handled by an intelligent assistant. This frees up your team's time for things like:

- Creative thinking
- Strategic planning
- Complex problem-solving

65% of workers say automating manual tasks reduces stress.

(continued on page 2)

Cloud-Based Collaboration

Cloud storage platforms allow teams to access and share documents seamlessly. No matter where they are or what time it is. This eliminates the need for emailing back-and-forth versions. It ensures everyone is working on the latest iteration.

Additionally, cloud-based collaboration tools enable real-time document editing, as well as communication, fostering efficient teamwork.

Communication Revolution

Gone are the days of phone tag and endless email chains. Instant messaging platforms and video conferencing tools provide instant communication channels. This facilitates quick questions, brainstorming sessions, and remote team collaboration.

Enhancing Accuracy: Technology Mitigates Errors

Technology saves time. But it also reduces errors that can derail projects and waste valuable resources. Here are some ways you can leverage tech to do this.

Data Accuracy Champions

Spreadsheet formulas automate calculations. This eliminates the risk of human error in manual data entry. Project management software tracks deadlines and dependencies. This ensures tasks stay on schedule and budgets are adhered to. These tools provide a single source of truth for project information. This eliminates confusion and miscommunication.

Data Analytics for Informed Decisions

Data analytics tools provide insights into:

- Customer behavior
- Marketing campaign performance
- Project progress

This data-driven approach allows teams to make informed decisions based on real-time information. Having insightful analytics reduces the risk of costly mistakes.

Fostering Teamwork: Technology Bridges the Communication Gap

Technology empowers effective communication and collaboration, essential for a productive team environment. Here's how it can do that.

Remote Work Enablement

Cloud-based tools and video conferencing apps promote seamless remote work. They allow teams to collaborate regardless of location. This fosters a more diverse workforce and expands your talent pool.

Knowledge Sharing Made Easy

Internal wikis and knowledge-sharing platforms allow teams to document processes. As well as share best practices and create a repository of company knowledge. This reduces the time spent reinventing the wheel. It also fosters a culture of learning and continuous improvement.

Project Management Made Simple

Collaborative project management tools provide many features, including:

- Clear task overviews
- Deadlines visibility
- Communication channels

This ensures everyone is on the same page. It fosters accountability and promotes smooth project execution.

Creating a Tech-Savvy Workspace: Considerations for Implementation

The benefits of technology in the office are undeniable. But successful implementation requires careful consideration.

Choose the Right Tools

Not all tech solutions are created equal. Review your specific needs. Choose tools that integrate seamlessly with your existing systems and workflows. User-friendliness is key. Complex tools can hinder productivity if they need extensive training.

Cybersecurity is Paramount

As your reliance on technology increases, so does the need for robust cybersecurity. Put in place data encryption and strong password protocols. Don't forget the importance of employee training on cybersecurity best practices.

Digital Divide Awareness

Ensure technology adoption doesn't leave anyone behind. Provide training and support for employees. Especially those who might be less comfortable with new tools. Remember, technology should empower everyone, not create barriers.

Embrace Change Management

Technology adoption isn't always easy. Be prepared to manage change within your team and provide ongoing support as they adapt to new tools and workflows. The extra help getting over road bumps can make a world of difference.

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

PHISHING 2.0:
HOW AI IS AMPLIFYING DANGER & WHAT YOU CAN DO

Phishing has always been a threat. Now, with AI, it's more dangerous than ever. Phishing 2.0 is here. It's smarter, more convincing, and harder to detect. A recent study found a 60% increase in AI-driven phishing attacks. This is a wake-up call that phishing is only getting worse.

Here's how AI amplifies the threat of phishing:

- Creating realistic messages
- Personalized attacks
- Better targeted spear phishing
- Phishing is automated
- Deepfake technology

The Impact of AI- Enhanced Phishing

- Increased Success Rates: AI makes phishing more effective. More people fall for these sophisticated attacks.
- Harder to Detect: Traditional phishing detection methods struggle against AI-enhanced attacks.
- Greater Damage: AI-enhanced phishing can cause more damage. Personalized attacks can lead to significant data breaches and the consequences.

How to Protect Yourself

- Be Skeptical: Always be skeptical of unsolicited messages. Don't click on links or download attachments from unknown sources.
- Check for Red Flags: Look for red flags in emails. Be cautious if the email seems too good to be true.
- Use Multi-Factor Authentication (MFA): MFA adds an extra layer of security.
- Educate Yourself and Others: Learn about AI phishing tactics.
- Use Advanced Security Tools: Invest in advanced security tools.
- Report Phishing Attempts: Report phishing attempts to your IT team or email provider.
- Enable Email Authentication: Use email authentication protocols like SPF, DKIM, and DMARC.
- Regular Security Audits: This helps identify vulnerabilities in your systems.

Gadget of the Month...

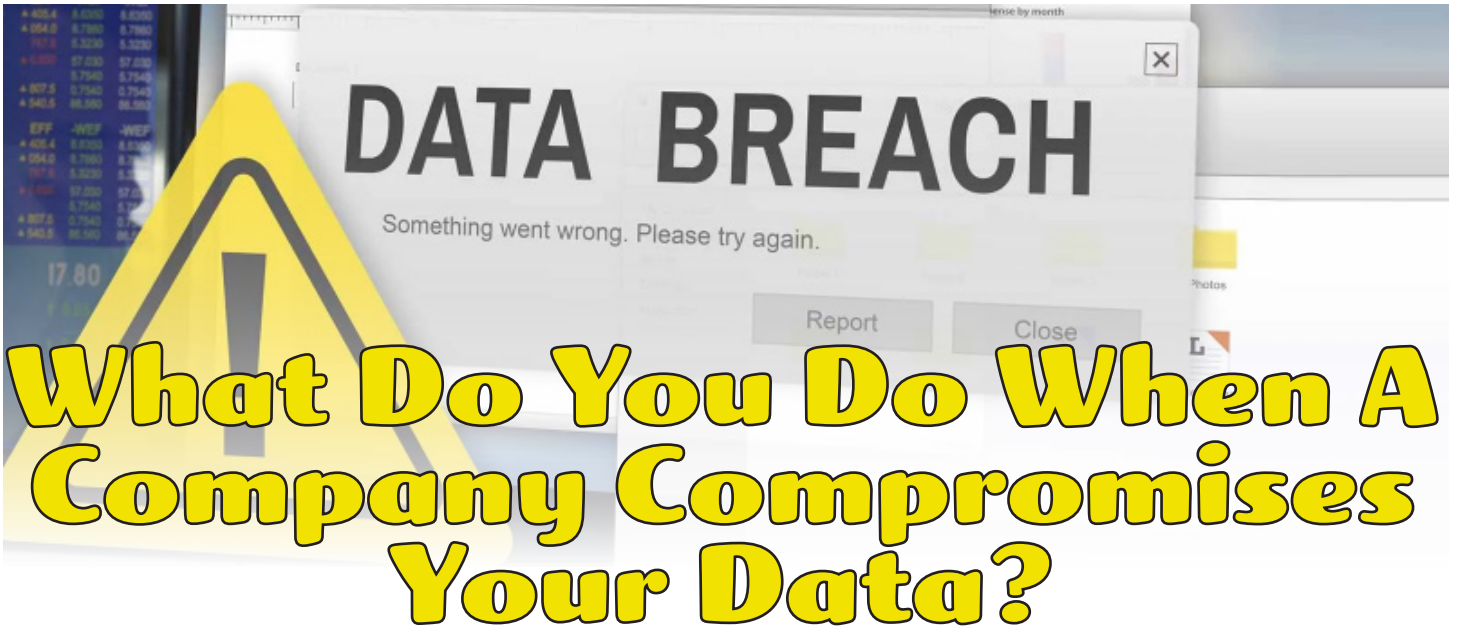
Logitech Casa Pop-Up Desk

The Casa Pop-Up Desk allows you to choose a comfortable and focused work area within your home.

When your workday is over, simply fold it away.

This compact kit includes a laptop stand, wireless keyboard, touchpad, and storage space—all neatly packed into a beautiful fabric case, available in three colors that complement your home decor.

Just $180 on Amazon!



What Do You Do When A Company Compromises Your Data?

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals.

When sensitive information leaks, you'll have to do some recon to protect your accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

What To Do After Your Data's Been Leaked

1. First, make sure the breach is legit

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen

After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts

Often, after data leaks, hackers use the information they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection

Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

Tech Giggles!

Why did the IT guy go to the hospital?

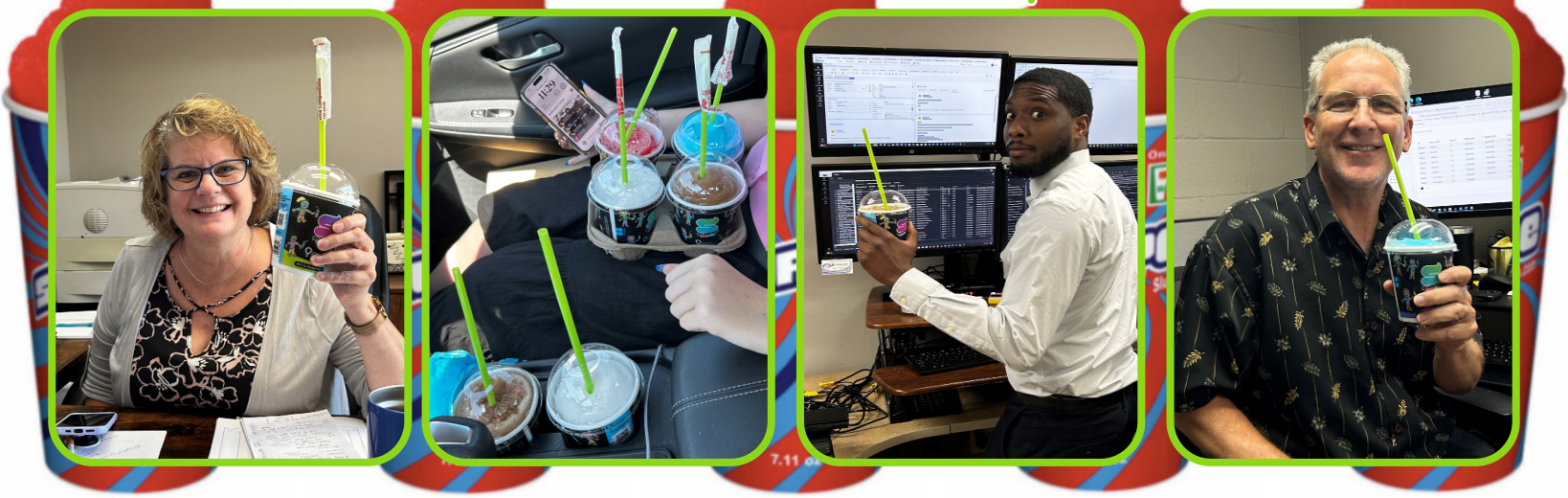
...

He touched the firewall!

What's NEW at CSU?

Slurpee Day at 7-Eleven

Free slurpees? CSU says, YES! Nina and Caitlyn went out on 7-Eleven day and hopped around to 3 different 7-Elevens to get all the CSU fam a free slurpee!



Lottery Day!

On National Lottery Day, we got everybody scratch-off tickets! Almost everyone won some cash! Melvin was the biggest winner of all with $20!

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

August Birthday!

Happy Birthday to our rock & rollin', regae-lovin', smooth-talkin', Mike! He has been with CSU for 26 years and is such an important member!

Give him a call and you'll find his chill voice and slight southern accent will rid you of your worries!

Happy Birthday Mike! Hope it's a gnarly one!

Chicken Wing Party!

It was National Chicken Wing Day 7/29! So obviously we had to order some Buffalo Wild Wings and enjoy getting our hands messy in some yummy chicken wings!

Caitlyn showing up strong in a BWW jersey!

After chowing on some wings, Byron tries to stay healthy with the celery!