Connection

May 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

Top 10 Security Tips for Mobile App Users

Mobile apps are an essential part of our daily lives, but they also expose us to risks from fraudsters who may steal information or damage our devices. Here's how to stay safe while using mobile apps.

How to Choose Safe Apps:

1. Download Only from Official Stores

Always download apps from trusted sources like the App Store or Google Play. Avoid third-party websites, as they might offer malicious versions of apps.

2. Check App Ratings and Reviews

Before downloading an app, take a look at the ratings and reviews from other users. This can give you an idea of the app's reliability and security.

(continued on page 2)

What to Do Before Installing an App:

3. Review App Permissions

Apps often ask for permission to access various parts of your phone. Consider whether the app really needs the information it's requesting, and only grant permissions that are essential for its functionality.

4. Update Your Phone's Operating System

Regular software updates help patch security vulnerabilities. Make sure your phone's OS is up-to-date to keep your device protected.

How to Protect Your Personal Information:

5. Use Strong Passwords

Create complex, unique passwords for each app. Avoid using the same password across multiple apps to reduce the risk of a security breach.

6. Enable Two-Factor Authentication

Two-factor authentication (2FA) adds an extra layer of security. It requires a second verification step, making it much harder for unauthorized users to access your accounts.

What to Be Careful About When Using Apps:

7. Avoid Public Wi-Fi

Public Wi-Fi networks are often not secure, so avoid using them for sensitive apps like banking or shopping. Use a trusted, private network whenever possible.

8. Log Out of Apps When Not in Use

Always log out of apps, especially those with personal or sensitive information, like banking or email apps. If your phone is lost or stolen, this will make it harder for someone to access your accounts.

How to Protect Your Apps:

9. Update Your Apps Regularly

App developers frequently release updates to fix security vulnerabilities. Make sure to update your apps whenever a new version is available to stay protected.

10. Use App Security Features

Many apps offer additional security features like fingerprint scanning or face recognition. Enable these features to add an extra layer of protection for your personal information.

CSU Can Cover You!:

While these tips are important for securing your mobile devices, managing mobile security can be a hassle. That's where CSU comes in.

We cover your mobile devices too, ensuring that all your devices are protected, so you don't have to worry about the details. With CSU, you can rest easy knowing that your mobile security is in expert hands!

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

THE U.S. CYBER TRUST MARK & WHY IT MATTERS

The Cyber Trust Mark is a new U.S. government label that shows a smart device has passed strict security testing.

- Devices with the mark meet national cybersecurity standards
- It helps you spot safer, more secure options at a glance
- No mark doesn't mean unsafe—but do your research!

Bottom line: The Cyber Trust Mark makes it easier to choose smart devices you can trust. Learn more at: https://www.fcc.gov/CyberTrustMark

Referrals...

Not the one's you get in school for causing trouble. We mean the good kind—where you share something great!

If you love working with our team and value our service of protecting and fixing your tech, help us grow by referring a friend, family member, or business neighbor who could benefit from our IT support.

What's a Good Referral?

- **Someone looking for IT support**
- **A business in the Washington, DC Metro area**
- **Interested in a free network assessment and IT proposal**

You don't need to worry about the details—just send us their contact info and we'll take it from there!

Gadget of the Month!

BENQ SCREENBAR

BenQ's ScreenBar, an LED monitor light, offers autodimming, a space-saving design, and USB power.

It lets you work comfortably without straining your eyes.

It provides 100% glare-free lighting and lasts up to 50,000 hours.

The ScreenBar supports adjustable brightness and color temperature, fitting all kinds of monitors up to 2.5 cm thick.

$179 on Amazon

IS YOUR BUSINESS HARDWARE HOLDING YOU BACK?

Your business hardware – your computers, printers, and other tech that keeps your day running smoothly – is easy to take for granted.

When they're working fine you don't give them much thought. But how often should you stop to think about whether they're performing at their best?

The truth is, properly maintaining your hardware is crucial for your business's success.

Just like a car needs regular servicing to keep running smoothly, your tech requires attention too. Dust can build up inside computers, slowing them down or even causing overheating.

And those software updates that seem like a hassle, are often designed to keep your devices working efficiently and securely. If your hardware isn't looked after, its performance will suffer, costing you time and money.

Sometimes, though, maintenance and repairs aren't enough.

If your hardware is old or outdated, it could be holding your business back. For example, older computers often struggle to run modern software, leading to frustrating delays and crashes. Worse still, outdated hardware can be a security risk, as it may not be compatible with the latest updates designed to protect you from cyber threats.

When deciding between repairing or replacing hardware, it's important to consider the bigger picture. While repairs might seem like a more affordable option initially, if your device is consistently slowing down productivity or breaking down, it could ultimately cost more in the long run. Investing in new equipment might seem like a significant expense, but it can save you both money and stress over time, while also giving your business a competitive edge. Think of it like a car: would you prefer to keep pouring money into fixing an old car, or would you rather invest that same money in a new one that runs smoothly and reliably?

Outdated hardware doesn't just affect performance; it can

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

also impact your team's morale and your customers' experience. No one enjoys battling with slow computers or unreliable printers.

Keeping your tech up to date makes sure everything runs smoothly, keeping your team happy and your business efficient.

Take a moment to assess your hardware. Is it performing well, or could it be time for an upgrade? Making the right investment now can save you both time and money down the road.

And if you haven't yet, it's the perfect time to check if your computers are ready for the upgrade to Windows 11.

Is it time for a hardware audit? We're here to help! Just reach out – we've got you covered.

Tech Giggles!

Why did the guy get fired from the keyboard factory?

...

He wasn't putting in enough Shifts!

Q&A

Q: What's the #1 cybersecurity threat to organizations today?

A: Internal employees! Even trusted team members can unknowingly put your organization at risk.

Q: How are employees causing security risks?

A: Often without realizing it—they might download unauthorized software, fall for phishing scams, click on malicious links, use weak passwords, or open infected files.

Q: Are they doing this on purpose?

A: Nope. Most employees aren't careless—they're just unaware of the risks. Education is key!

Q: How do we reduce these risks?

A: CSU offers weekly cybersecurity training! This includes short training videos and examples. Also includes mock phishing attacks sent to your email for real-world practice.

Q: Why are these important?

A: They help employees experience first-hand how easy it is to fall for a scam. Building awareness creates stronger habits and a more secure workplace.

What's NEW at CSU?

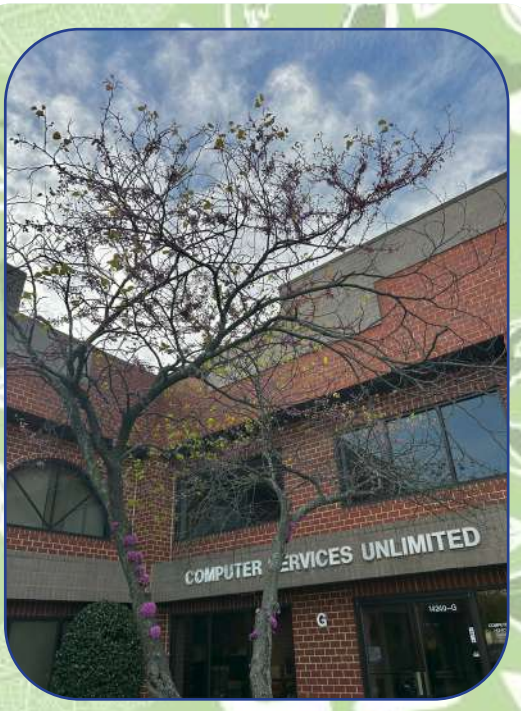
April Fools Day!

There's a semi-unspoken rule, "don't prank the boss." But for April Fools Day, Caitlyn had to prank the boss a little bit. Notice anything unusual about the computer monitors?

SOMETHING ABOUT ALASKA: THEY HAVE EARTHQUAKES! OUR TECH, WILL, HAD A BIT OF A SHAKE IN LATE APRIL!

Notice Anything Odd?

Maybe the tiny detail that Lexi, a small dog with big audacity, has chosen to plop herself smack in the middle of Faye's seat—completely ignoring the many other cozy options available. Poor Faye... hard being a big dog in a small dog's world.



Happy Earth Day!

A beautiful sunrise, warm breezy day, and trees turning green. A lovely Earth Day at CSU :)

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

May Birthday!

Happy Birthday Adam! Your chipper personality and goofy pranks brighten the office! And to add to that, the helpful IT assistance and expert tech videos you make are supurb! Hope you have an awesome day!

Sibling Day!

Can you guess which one is Michelle?

EXERCISE DAY!

Caitlyn had the staff do a little bit of exercise to start the work day! Paola was a beast doing both the pushup challenge and the squat challenge. Melvin finished the pushups 1st with both good speed and form, old muscles for the win!