CSU Connection
Serving our community for over 30 years
July 2023

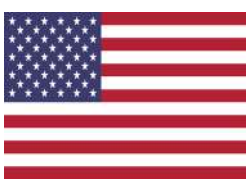
Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity. and profitability.

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

in this issue...

"FOR WHAT AVAIL THE PLOUGH OR SAIL, OR LAND OR LIFE, IF FREEDOM FAIL?"

~RALPH WALDO EMERSON



Is Your Shopping App Invading Your Privacy?

Online shopping has become a common activity for many people and businesses. It's convenient, easy, and allows us to buy items from the comfort of our homes. But with the rise of online shopping, there are concerns about privacy and security.

Not all shopping apps are created equally. Often people get excited and install an app without checking privacy practices. Apps can collect more data from your smartphone than you realize. Whether you use your phone for personal use, business use, or both, your data can be at risk.

So can your privacy.

Shady Data Collection Practices from Popular Shopping App SHEIN

Recently, security experts found a popular shopping app spying on users' copy-and-paste activity. This app was tracking users' keystrokes, screenshots, and even their GPS location. This raises the question: Is your online shopping app invading your privacy?

SHEIN is the app in question, and it's a popular shopping app with millions of users. According to reports, researchers found the app collecting data from users' clipboards. This included any text that users copied and pasted. This means that if the user copied and pasted sensitive information, the app would have access to it.

Including things like passwords or credit card numbers.

Not only that but the app was also found to be tracking users' GPS location. SHEIN was also collecting data from device sensors, including the accelerometer and gyroscope. This means that the app was able to track users' movements. As well as collecting information about how they were using their device.

The app's developers claimed that the data collection was for "optimizing user experience." A very vague explanation that's used by other app developers as well.

The developers stated that the collected data was only used for internal purposes. But this explanation wasn't enough to please privacy experts. Those experts raised concerns about the app's data collection practices.

cont. on pg 2

Temu Data Collection Practices Questioned

This isn't the first time people caught an app grabbing data without users' knowledge. Many popular apps collect data from their users, often for targeted advertising purposes.

The popularity of the shopping app Temu has been exploding recently. Since the app appeared in a Superbowl Ad in 2023, people have been flocking to it.

But Temu is another shopping app with questionable data collection practices. Some of the data that Temu collects includes:

-Your name, address, phone number
-Details you enter, like birthday, photo, and social profiles
-Your phone's operating system and version
-Your IP address and GPS location (if enabled)
-Your browsing data

Tips to Protect Your Privacy When Using Shopping Apps:

Know What You're Getting Into (Read the Privacy Policy)

Yes, it's hard to stop and read a long privacy policy. But, if you don't, you could end up sharing a lot more than you realize.

Turn Off Sharing Features

Turn off any data-sharing features you don't need in your phone's settings.

Such as location services. Most smartphones allow you to choose which apps you want to use it with.

Research Apps Before You Download

It's easy to get caught up in a fad. You hear your friend talk about an app, and you want to check it out. But it pays to research before you download.

Shop on a Website Instead

You can limit the dangerous data collection of shopping apps by using a website instead. Most legitimate companies have an official website.

Remove Apps You Don't Use

If you're not using the app regularly, remove it from your phone. Having unused apps on your phone is a big risk.

How To Stay Safe on Social Media: A Series

Part 2: YouTube

While it's unlikely you'll ever get a YouTube virus from watching videos, real dangers exist on the site. Cybercriminals trick us into clicking links so they can install malicious software on our devices. Falling for such nefarious traps is easier than you think.

Here are some good rules to follow:

- **Avoid clicking video description links**
- **Beware the YouTube comments section**
- **Video ads can lead you astray**
- **Enable YouTube Restricted Mode for Kids and Download the YouTube Kids App**

Artificial Intelligence also gets in on the act... A.I. generated YouTube Video Tutorials spread a variety of stealer malware such as Raccoon, RedLine, and Vidar. The videos lure users by pretending to be tutorials on downloading cracked software versions such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other licensed products available only to paid users.

YouTube

Sources and additional information:

•**Can you get a YouTube virus?** (https://www.pandasecurity.com/en/mediacenter/mobile-news/youtube-virus-tips/)
•**Warning: AI-generated YouTube Video Tutorials Spreading Infostealer Malware** (https://thehackernews.com/2023/03/warning-ai-generated-youtube-video.html)

Travel Safety and Security Tips ...because Hackers Don't Take a Vacation!

Who doesn't love a nice and refreshing summer vacation?! It feels good to plan an adventure, to get away, relax and enjoy new places and experiences.

One thing we know, *hackers don't take a vacation*, and they are excited that you may let your guard down as you unwind and forget about the challenges back home.

Here are some helpful tips:

- Travel lightly and limit the devices you take with you
- Check the privacy and security settings and limit how much information you are sharing
- Set up the "Find My Phone" feature to remotely wipe your data if it is lost or stolen.
- Password protect all devices with unique, secure passwords
- Update your software to get the most recent security updates
- Back-Up your files in case you lose a device and need to recover the data when back home.

Scams:

Be Cautious When Booking Hotels and Travel

Book directly with a known online booking company and access by typing in their address rather than using a link in an email. Hackers are creating look-alike websites that can steal your information, including credit card numbers.

If a booking agent calls you out of the blue, they may be a scammer. Hang up and call the property directly.

Hotel and Airline points can be targeted by scammers who send random emails advising that you log in and reset your password. Go directly to your account and check your account. If 2-factor authentication is available, take advantage of the extra security. Never pay by wire transfer, cryptocurrency, or gift cards, which you often will not be able to get back.

Be Cautious of Clicking Links in Travel Promotion Emails

Hover over links to be sure they are going where they say they are going. Be extra cautious when using your cell phone because you can't hover over links to check them. Use credit cards rather than debit cards because they offer better fraud protection. If it sounds too good to be true, it probably is! Confirm your reservations directly with the hotel or airline.
TSA Pre-check and COVID-testing phishing emails are rampant, so think before you click and give them your information.

Good Advice to Consider:

Stop auto-connecting: Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to. If you do not need them, switch them off.

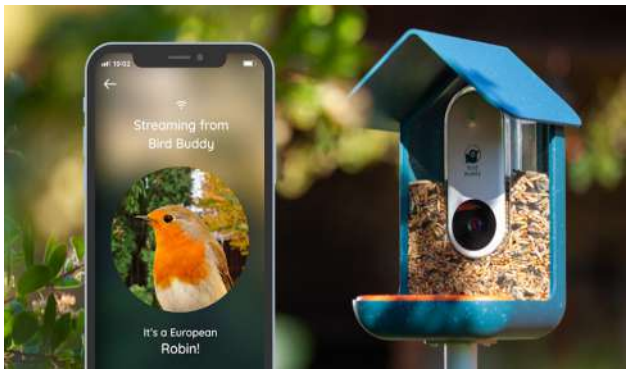
Protect your credit, debit, identification, and money cards from electronic fraud: RFID (Radio-frequency identification uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver, and a transmitter) devices can scan your pocket or purse to steal your card's information. RDIF-blocking sleeves and wallets are readily available.

Tourist Visa: If you need a tourist Visa to travel to a specific country, get it from the country itself, don't go through a third party, even if they advertise an expedited time. They are probably looking for your sensitive information, your money, and you probably won't get it. (AARP) To see if you need a Visa to travel: https://www.atlys.com/post/countries-where-us-citizens-need-a-visa

From the National Cybersecurity Alliance: Planes, Trains, Automobiles...
Staying Safe Online Webinar (StaySafeOnline.org)

We highly recommend this webinar which will provide practical tips for maintaining your amazing cybersecurity habits even when you are away from home! Learn about public wi-fi, when to use your device's location settings, and keeping your identity safe when traveling. It doesn't matter if you're headed across an ocean or down the street, this information will give you a better understanding of how to best protect yourself when you're on the go.
(https://www.youtube.com/watch?v=ck8c8PgGySU&t=143s)

Gadget of the Month:



Bird Buddy
Smart Bird Feeder

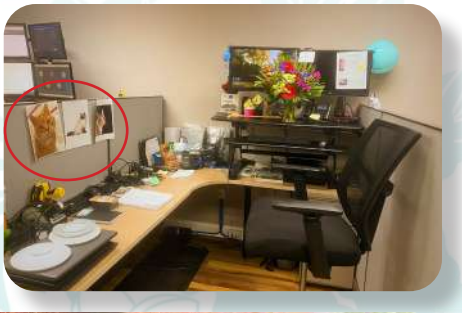
Meet the AI-powered camera bird feeder that notifies you of feathered visitors, takes their photos, and organizes them into a beautiful collection to admire and easily share with your friends and family!

Get yours today at
www.mybirdbuddy.com

(continued on pg 5)

Chuck's Birthday Celebration~
It Was a Blast!

Thank you to all who helped us celebrate Chuck for his big 6-0! We had friends, family, clients, employees, and past employees gather for a day in what felt like our own personal Hawaii! (Kind of...)



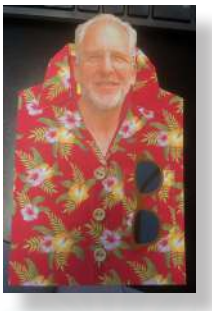
Chuck's first surprise... everyone wearing their favorite hawaiian shirt. You can call it a staycation.

From Chuck having a fun decorated office space (with pictures of his favorite animal, cats, of course), to ha-waiian shirts, Willard's BBQ, and corn hole in the parking lot, this oridnary Tuesday was filled with teamwork, surprises, and lots of laughter.

#teamwork

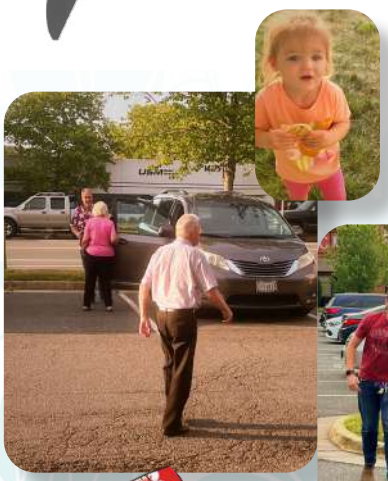
June 13th, 2023

Chuck's new side hustle- modeling for birthday cards!



Almost.

Good people, good talks, good times!



GOOD FOOD·

We hope you had an awesome day and know how much you rock, Chuck!

The celebrations continued on Wednesday when Chuck received a money tree! (Perks of owning your own business- turns out money does grow on trees)

Just kidding!

Where would our IT be without you?!

What's Happening at CSU?

The Sherman's latest endeavor... Chicken Raising.

Lots of eggs!

(Feisty)

It's safe to say that the Sherman's have embraced the country lifestyle.

Introducing... the 6 Red Hybrid Sherman Hens:

- Mama/Fluffy - (Biggest and boldest colors!)
- Alberta -(May be deaf; has 1 goblet out of 2; appreciates personal space)
- Feisty- (Proudly lives up to her name- she pecks at feet and doesn't go where she is led...)
- Frizzle - (Part of the twin duo with Feisty, has lots of feathers)
- Gertrude- (Has dark neck feathers)
- Sprinkle- (Has white dots all over)

-The hens were 18 weeks old when they were first adpoted. (Already full grown and laying eggs)
-They each lay 1 egg per day, in the same spot! (That's 1/2 a dozen each day on the Sherman "farm".)
-They are losing their feathers through a process called moulting- a yearly shedding of their old feathers. (Fresh feathers and fresh eggs!! Woo hoo!)
-They are also digging lots of holes to eat some delicious bugs. Yum!

For now, the hens are 20 weeks old, adjusting to their new routine, and are loving the fresh country air! This has been a learning experience for everyone. Stay tuned to hear periodic updates on the hens and their great service!

Introducing... Client Comments

We weant to hear from you, our clients, and include your answers in the next newsletter! Send your answers to Emily at echona@csuinc.com by Wednesday July 26th to be featured in next month's letter!

-What is an endeavor/hobby you've been wanting to take on?
-What is your first step to getting started?

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

Get connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Coffee Break:
www.csuinc.com/coffee

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