Willow Valley Computer Club

September, 2025 | Newsletter | Volume 26, Issue 5

Programs are at 2:00 pm the first Thursday of the month (except July-August) in the Cultural Center unless otherwise noted.

Inside this issue:

- Summary of Project Upskill II Presentation on 3/25/2025
- The Internet Of Things
- CCTC Bi-Monthly Report
- Volunteer Opportunities

Computer Club Leadership

- President: Al Williams
- Vice President: open
- Secretary: Paula Sandridge
- Treasurer: Lee Wermuth
- Previous President: Sid Paskowitz

Committee Chairpersons

- Club Website: Paula Sandridge
- Computer Room: Lee Wermuth
- Information Central: Sid Paskowitz
- Newsletter: Mike Pancione
- Programs: Bill Huddleston
- Publicity: open
- Smart Life: Al Fulvio
- Training: Bill Skelly

Director

- CCTC: John Santora

Advisors

- Bruce Mawson
- Tony Poulos
- Cathy Thorn

President's Pen

by Al Williams

As we go into the Fall, the Willow Valley Computer Club continues to provide education, general information, and help to residents.

We also continue to receive requests for help from residents who been scammed, and as a result have lost money to the scammers.

I encourage you to read the recent "Be on the Alert for Scammers" notice sent to all Computer Club members. The best defense is to be aware of ways that scammers attack.

I also suggest that you take one of our classes to learn more, or read reputable websites such as arstechnica.com or bleepingcomputer.com

Contact Information

For more information about the Computer Club, please contact Al Williams via email at wvcomputerclub@gmail.com.

Please keep your email address on Club records current so we can send you important emails. Send email corrections or updates to Lee Wermuth at lwermuth582@gmail.com.

Bill Skelly is the Willow Valley Computer Club Training Coordinator. We are always looking for residents qualified to teach computer-related topics. We want our classes to support your needs. Contact Bill (whskelly@aol.com) to volunteer or to offer ideas on topics needed.

NOTE: The Computer Club Technology Center (CCTC) is open on Thursdays only, from 10 am to 4 pm. The CCTC is located on the 5th floor of Manor North 'J 'building. The door may be closed, but with a sign indicating *Please Knock.*

Apple Items Available: See Bruce Thompson in the CCTC.

Project Upskill II Series Presentations

Introduction

The Project Upskill II series of presentations is devoted to helping people protect their personal information from cybercriminals' theft. The most consequential information is financial or highly personal, and it is stored on home computers, cell phones, vehicle systems, and legitimate internet websites. Of course, it can also be on fraudulent sites that users may unwittingly be lured to use.

Cybercriminals pose real threats, and defending against them requires constant vigilance. Unfortunately, being vigilant takes effort, and most people prefer not to or lack the skill to devote time to it. The Upskill series discusses protective measures that require little effort but offer excellent protection if implemented well. Of course, the Computer Club provides help to residents who lack basic skills.

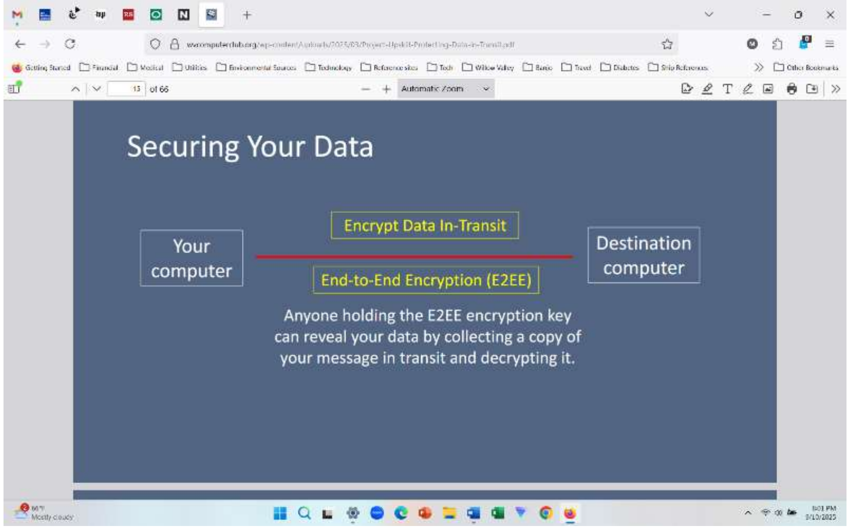
The eight Upskill presentations were given over four months, and for those who missed some or all, this Newsletter will attempt to summarize the key points of each presentation. The current presentations are available at **wvcomputerclub.org.** The summaries will try to elaborate on the points in the presentations, which were explained in detail by the Computer Club speakers: Al Williams, Cathy Thorn, and Tony Paulos. The first two presentations were summarized in our last Newsletter. The next is summarized below.

How to Protect Your Data In Transit (from Upskill Presentation on 3/25)

The data on your PC, cell phone and even your car is particularly vulnerable to cybercriminals whether you are home or travelling. This presentation identifies the key elements for protecting your data while you and/or it travel.

- Encryption the basis for secure communication
- Communicate securely on your mobile device
- Stay safe while web surfing: Browser settings
- Stay safe while web surfing: Accessing websites securely
- Get the most out of cloud storage and services while minimizing the risk

Encryption: The basis for secure communication. Encryption involves the encoding data or a message with a complex set of rules so that only those people, or applications, that have a unique key are able to read it. This diagram depicts how an encrypted transmission between two computers works.



Securing Your Data

Your computer

Encrypt Data In-Transit

End-to-End Encryption (E2EE)

Destination computer

Anyone holding the E2EE encryption key can reveal your data by collecting a copy of your message in transit and decrypting it.

Communicate Securely on Your Mobile Device

- o Use a properly vetted secure messaging app with end-to-end encryption that provides functionality for text messages and phone calls.
  - The Problem: Text messages and voice calls are vulnerable to interception by threat actors.
    - ✓ 5G networks provide encryption for calls and data, but carriers may downgrade 5G connections to 4G, 3G, or 2G to manage capacity, which do not offer encryption.
    - ✓ Traditional cell phone calls are vulnerable to interception.
    - ✓ Data communications that do not use encryption are vulnerable
    - ✓ Email messages sent from your phone's email app or browser may be intercepted by a threat actor
    - ✓ Email service providers may provide a form of encryption to protect data traveling across their own network system (Gmail to Gmail) but are unable to ensure its security when transmitted to a different email service provider.
  - The Solution: Use a secure messaging app for texting and calling on your mobile device. It must have support for:
    - ✓ end-to-end encryption
    - ✓ Multi-factor Authentication (MFA)
    - ✓ text messages, including group chats and disappearing messages
  - Partial Solutions:
    - ✓ Apple's iMessages provides end-to-end encryption only when you are communicating with other iOS users. Messages sent to non-iOS users are not encrypted.
    - ✓ Google's Messages provide end-to-end encryption with other Google Messages users, but not with users from other services.
  - Recommended Solution: Get SIGNAL. Information available at SIGNAL.ORG
- o Place sensitive information in an encrypted file attachment when you send emails**.**

Stay Safe While Surfing – Browser Settings

The problem: Treat actors can exploit vulnerabilities in web browsers and web browsers collect a lot of personal information which can be used by these criminals and data brokers.

- A website may ask permission to access
  - ✓ Geolocation data
  - ✓ Camera
  - ✓ Microphone
- A website might ask permission to send pop-up notifications which can be used in phishing campaigns.
- Third-party cookies collect, store, and share information
  - ✓ Website history
  - ✓ Search history
  - ✓ The links you clicked on
  - ✓ The content you interact with on social media, and more
  - ✓ Data brokers and advertisers often use third-party cookies to compile and sell your information.
- Browsers themselves store data
  - ✓ Browsing history
  - ✓ Saved form data (personal data to autofill information)

- ✓ Location data (uses IP address, Wi-Fi, and Bluetooth
- ✓ Account credentials (if you allow the browser to store them)
- ✓ Download history (and the path to where every file is stored)
- ✓ Personal data (browsing habits and device activity)

The Solution: Protect yourself against malware

- Keep your browser up to date (Enable automatic updates, if available)
- Restart your browser regularly to allow updates to take effect
- If you are accessing your browser account (Chrome, Edge, …) enable multi-factor authentication to protect your browser account.
- Manage the advertising settings in your browser to limit access to some of your browser's stored data
- Turn off ad personalization
- Limit the amount of data that websites and third parties can obtain through your browser:
- Block third-party cookies in your browser settings
- Clear third-party cookies already stored (this will remove all your cookies requiring you to re-enter some information)
- Restart your browser regularly to allow updates to take effect
- Restrict site permissions as much as possible:
- Do not give websites access to your location, camera, or microphone unless required for the website to function properly.
- Properly vet browser extensions
- Use AdBlock
- Browser Settings: Use the USSOCOM's Social Media Smart Cards for instructions for changing the browser settings of some of the most popular browsers. The link to the instructions is https://www.socom.mil/documents/ussocomsocialmediasmartcards.pdf

Stay safe while web surfing: Accessing websites securely

The Problem: If the website's URL does not include https://, anyone with technical knowledge can view the data you share with the website.

The Solution: Only access websites that use https://. To avoid accidental connections to http:// websites, change your preference in your browser settings to allow only HTTPS connections

- Verify the website's URL by looking for slight changes from the desired URL.
- Note that a threat actor can still see which website you are accessing, but they cannot see your content.

Get the most out of cloud storage and services while minimizing the risk

The Problem: You may lose important data while using your computer. Cloud services offer complementary storage for your critical data.

Benefits and Risks of Cloud Storage:

- There is a potential for data to be lost.
- If you store your data only in the cloud and don't save a local copy, cyber incidents such as a denial-of-service attack could lead to the temporary or even permanent loss of your data

- Less control over your data. Your data is stored on servers you do not control. If the servers are located in another country, that country may require the cloud service to disclose your data.
- Scheduled server maintenance may prevent access to your data.
- Note that your data is probably encrypted but the service can be compelled to disclose your data if the service holds the encryption keys.
- Ensure that these services encrypt your data and are headquartered in a country with privacy and security laws that help protect your data.

The Internet of Things

By
David Della-Villa
Assistant Professor of Law, University of South Carolina
(Reprinted with Permission)

Some unusual witnesses helped convict Alex Murdaugh of the murders of his wife, Maggie, and son, Paul.

The first was Bubba, Maggie's yellow Labrador retriever. Prosecutors used a recording of Bubba to place Alex at the site of the murders. Given Alex's presence at the crime scene, other witnesses then revealed his movements, tracked his speed and explained what he had in his hands. Those other witnesses were a 2021 Chevy Suburban and Maggie, Paul and Alex's cellphones, which all provided data. They're all part of the Internet of Things, also known as IoT.

The privacy implications of devices connected to the internet are not often the most important consideration in solving a murder case. But outside of criminal prosecution, they affect people's privacy in ways that should give everyone pause.

The Internet of Things

The Internet of Things includes any object or device that automatically sends and receives data via the internet. When you use your phone to message someone or social media to post something, the sharing is deliberate. But the automatic nature of connected devices effectively cuts humans out of the loop. The data from these devices can reveal a lot about the people who interact with them – and about other people around the devices.

As an assistant professor of law at the University of South Carolina, I have watched as new kinds of connected devices have entered the market. New devices mean new ways to collect data about people.

Connected devices collect information from different contexts. Take your refrigerator. As a non-IoT device, your fridge generated no data about your kitchen, your food or how often you peeked inside. Your relationship with the fridge was effectively private. Only you knew about that midnight snack or whether you ogled a co-worker's lunch.

Now, smart refrigerators can respond to voice commands, show images of the items in your fridge, track who opens it, suggest recipes, generate grocery lists and even contact your car to let you know the milk has expired. All these functions require continuous streams of data.

Internet of Things devices such as smart refrigerators collect a lot of information. PonyWang/iStock via Getty Images

Device data and your privacy

Connected devices generate lots of data in contexts that have typically produced little data to make those situations “legible” to whoever can access the data.

In the past, if you wanted to monitor your heart rate, blood oxygenation, sleep patterns and stress levels, you might have undergone a battery of tests at a hospital. Specialized equipment in a controlled setting would have measured your body and make these parts of you visible to highly trained, licensed professionals. But now, devices such as the Oura Ring track and analyze all that information continuously, in non-health care contexts.

Even if you don’t mind sharing data with an Internet of Things company, there are privacy risks to using a device like this. In the health care context, a series of rules enforced by several groups make sure that connected equipment and the data the equipment generates have adequate cybersecurity protections. Away from that context, connected devices that perform similar functions don’t have to meet the same cybersecurity standards.

The U.S. Cyber Trust Mark program, administered by the Federal Communications Commission, is developing cybersecurity standards for Internet of Things devices. But the program is voluntary. In some states, such as Washington, state laws set standards for protecting health data from connected devices. But these laws don’t cover all data from all devices in all contexts. This leaves the devices, and the data they generate, particularly vulnerable to unwanted access by hackers.

Your inability to control who sees the data that connected devices gather is another privacy risk. It can give advertisers insights about potential customers. Absent a mandated opt-out, each device provider can decide what it does with customer data. Amazon, for example, recently removed the “Do Not Send Voice Recordings” option from the privacy settings of its popular smart speaker, Alexa.

Some connected-device providers participate in data markets, selling your data to the highest bidder. Sometimes those purchasers include government agencies. So, instead of needing a warrant to track your whereabouts or learn about activity in your home, they can purchase or access Internet of Things records.

A connected device can also compromise the data privacy of someone who just happens to be nearby.

Connected cars

Cars have joined the ranks of the Internet of Things. The 2021 Chevy Suburban that helped convict Alex Murdaugh simply tracked information about the vehicle. This included the vehicle’s speed, the turning radius of the steering wheel and time stamps.

Most modern vehicles also incorporate data from external sources. GPS data and infotainment systems that connect to cellphones also track the vehicle's movements. All of this data can also be used to track the whereabouts and behavior of drivers and other people in the vehicles.

The familiar shark fin antenna on modern cars does more than just pick up radio stations. It can also transmit data about you and your surroundings. Roman Vyshnikov/iStock via Getty Images

And as vehicles become increasingly automated, they need to make driving decisions in increasingly complex situations. To make safe driving decisions, they need data about the world around them. They need to know the size, speed and behavior of all the nearby vehicles on the roadway, moment to moment. They need to instantly identify the best way to avoid a pedestrian, cyclist or other object entering the roadway.

If you and I are driving in separate cars on the same roadway, it means my car is collecting information about you. And if my vehicle is connected, then data about you is being shared with other cars and car companies. In other words, if a Tesla had been present at the scene of the Murdaugh murders, its outward facing cameras could have captured footage. Bubba's testimony might not have been necessary.

Spillover data collection

Internet of Things devices generate data from similar situations in a highly structured way. Therefore, what data collectors learn about me from my connected device may also give them insights about someone else in a similar situation.

Take smart meters that share information with the water utility every 15 minutes. Imagine a subdivision with a narrow range of house and yard sizes. Water usage should be relatively comparable for each household. Data from even just a couple of houses can give a good sense of what water use should be for everyone in the neighborhood. Without actually collecting data from each house, data from connected devices reveals potentially private information about similarly situated people.

Data from IoT devices can also fuel insights into people who never use or make contact with these devices. Aggregated data from Oura rings, for instance, could contribute to decisions a health insurer makes about you.

Wearable devices like the Oura Ring collect information such as heart rate, temperature, oxygen saturation, and movement and breathing patterns. T3/Future via Getty Images

Connected devices are also changing. In addition to collecting data about the person using the device, a growing number of sensors collect information about the environment around that person.

Some of my research has examined what privacy means for people observed by vehicle sensor systems such as radar, lidar and sonar. These technologies capture potentially very revealing information about people and their property. Even the most comprehensive privacy laws in the United States offer people little recourse for the impact to their privacy.

Civilian drones are capable of gathering data about other people. But people observed by drones would have a tough time learning that data about them exists and an even harder time controlling how that information might be used.

Meanwhile, artificial intelligence systems are expanding the ways Internet of Things data can affect the privacy of other people by automating the process of training IoT systems. AI chipmaker Nvidia has created a digital environment, or model, where people can upload their connected device data. This environment can help train IoT devices to “predict the outcomes of the device’s interactions with other people,” according to Nvidia.

Models like this make it easy for AI devices that you don’t own to collect data or reach conclusions about you. In other words, IoT data processed by AI can make inferences about you, rendering you legible to the AI system even before you interact with an IoT device.

Looking forward

Internet of Things devices and the data they generate are here to stay. As the world becomes increasingly automated, I believe it’s important to be more aware of the way connected devices may be affecting people’s privacy.

The story of how vehicle data combined with cell data in the Murdaugh trial is a case in point. At the start of the trial, prosecutors came ready to show “phone call logs and texts, steps recorded, apps asking for information, GPS locations, changes when the phone went from vertical portrait mode to horizontal landscape mode and back, and — key to the prosecution’s case — when the camera was activated.”

But that was probably not enough to merit a conviction. During the trial, GM called and said something like “oh wait, we found something,” according to the prosecution. That vehicle data, combined with the cellphone data, told a story that Alex Murdaugh could not deny.

There are at least two lessons from this story. First, not even GM fully realized all the data it had collected in its vehicles. It’s important to be aware of just how much information IoT devices are collecting. Second, combining data from different IoT devices revealed incontestable details of Alex Murdaugh’s activities. Away from criminal court, combining data from multiple IoT devices can have a profound effect on people’s privacy.

If people’s data privacy matters, how do we address this reality? One way of potentially protecting people’s privacy is to make sure people and communities observed by connected devices have a direct say in what data the devices collect and how the data is used.

The article originally appeared here:
https://theconversation.com/how-internet-of-things-devices-affect-your-privacy-even-when-theyre-not-yours-251592

COMPUTER CLUB TECHNOLOGY CENTER RESIDENT SUPPORT REPORT

The CCTC, along with Computer Club volunteers, provide a range of information technology services to residents, practically on a daily basis. On Thursdays, the Center is open for resident visits. Daily, volunteers help residents with technology issues in residents homes. This report details these services.

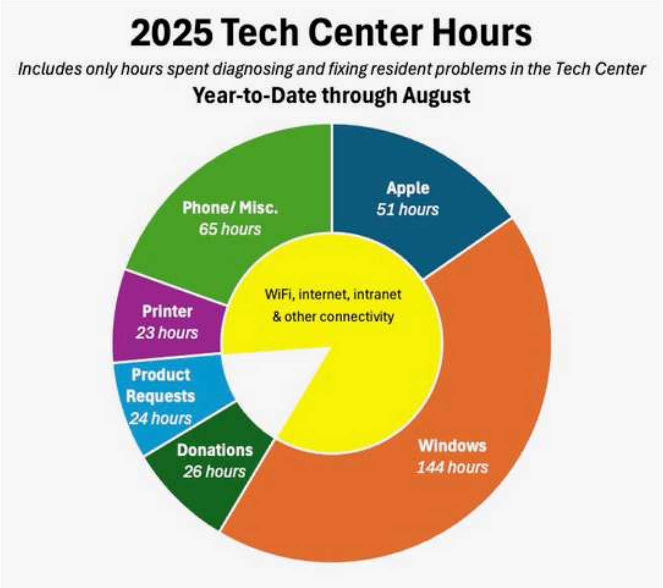
Hours – Thursdays 10am – 4pm (sometimes 9:30am – 5pm)
For the period July/August, 2025

- Open days – 8
- Active volunteer hours in CCTC – approximately 210
- Active WVCC volunteer hours outside CCTC – unknown
- Active current CCTC volunteers – 5 technical; 5 administrative (2 technical inactive)

Resident interactions: July & August, 2025

- Visits to CCTC – 89
  - ✓ Apple issues – 28
  - ✓ Windows issues – 26
  - ✓ Printer Issues – 3
  - ✓ Phone/Miscellaneous – 8
  - ✓ Donations – 20
  - ✓ Product Requests – 4
  - ✓ Known phone calls from/to residents – approximately 25
  - ✓ Known visits to resident's locations – approximately 20
  - ✓ Printer/scanner setup and connectivity issues
  - ✓ Connectivity issues, including TiVo and log-on security issues
  - ✓ Transfer data from old to new desktop PCs

Year-to-Date CCTC Activity: This chart summarizes the year-to-date approximate hours spent by CCTC volunteers in the Center. It does not include time spent in residents' apartments by either CCTC or Get Help volunteers.



Willow Valley Computer Club
Volunteer Opportunity

Volunteer Position Title: Deputy CCTC Director

Description of Role: The Deputy CCTC Director assists the CCTC Director as needed to accomplish the objectives set forth by the Willow Valley Computer Club's Executive Committee.

Training: The CCTC Director will provide training as needed for the Deputy CCTC Director to successfully accomplish their assignments.

Reporting: The Deputy CCTC Director will report to the CCTC Director.

Time Commitment: A minimum of four hours per week is needed. The candidate must be able to work during hours acceptable to the CCTC Director

Qualifications: Prior operations experience is desirable. A willingness to learn is imperative.

Do you have a question or want to provide feedback?
Please get in touch with us at wvcomputerclub@gmail.com

WVCC mission: "to provide the means to educate beginners or interested non-users on how to use a computer"

WVCC mission: "to provide a forum for interchange of computer information among members"

WVCC mission: "to arrange for speakers to talk about subjects of interest to those with some background and experience in computer use"