Willow Valley Computer Club

September 2022 | Newsletter | Volume 23, 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:(Click link below)

Computer Club Leadership

- President: Al Williams
- Vice President:Susan Culbertson
- Secretary: Gary Staton
- Treasurer: Lee Wermuth
- Previous President: Sid Paskowitz

Committee Chairpersons

- Program: Susan Culbertson
- Training: Chuck Smith
- Equipment: Cathy Thorn
- Technical Support: Tony Poulos
- Website: Sid Paskowitz
- Publicity: Ann Willets
- Newsletter: Susan Culbertson
- Apple SIG: Dick Beidleman
- Computer Lab: Lee Wermuth

Community Representatives

- Lakes Manor: Bruce Mawson
- Smart Life: Al Fulvio
- Garden Apartments: Al Williams
- Spring Run: Bob Scala

President's Pen *by Al Williams*

In this issue, we introduce two columns: *How-to Corner* and *Security News*. The columns offer selected articles from the web such as *Why Paper Receipts are Money at the Drive-Thru*, *Getting Older? Here's How to Make Windows More Comfortable* and *What to Do if You Drop your Smartphone in the Ocean.*

The first *Discovery* article, *Privacy and Anonymity*, was published in the July issue. That article explained privacy and anonymity at the conceptual level. In this issue the second *Discovery* article, *Privacy and Anonymity - Strategies*, will help you decide how to put privacy and anonymity into practice. Lists of resources for the two articles are also included in this issue.

Do you use Linux? Are you curious about Linux? We'd like to start a Linux Special Interest Group. If you're interested, please contact me at wvcomputerclub@gmail.com.

We recently learned that because we provide education; we work on computing devices; and because those computers may have valuable information, that we should obtain insurance. We verified this need with two additional attorneys. As a result, we have obtained these policies:

Directors and Officers
Technology Errors and Omissions
General Liability

Our Technology Errors and Omissions insurance requires us to charge a fee for service for working on computing devices or providing advice. We decided to include that fee in all new membership dues. We are also retroactively providing this benefit at no additional cost to current members.

The Computer Club has many volunteers willing to help you with your computer problem. You'll find the list at https://resident.willowvalley.org/cclub/gethelp.aspx.

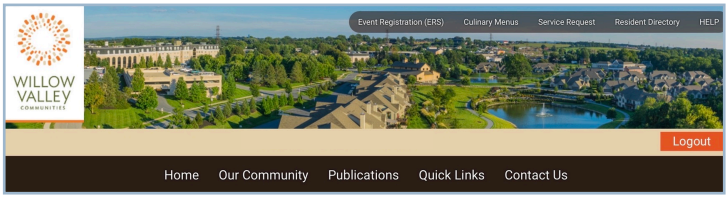
The Willow Valley Computer Club provides presentations of general interest, courses for specific topics, time-critical alerts, and this newsletter. We also provide past presentations and other computer related information on the Computer Club's Information Central, as you would expect. But we also provide a wide range of information for residents on Information Central that is not computer-related. I encourage you to check Information Central out. You'll find it on the resident intranet.

The newsletter is issued every other month which makes the newsletter ideally suited for articles that readers may want to read and consider. When an article has been presented three times, it is retired.

If you would like to present, teach or be involved in some other way in the Computer Club, please let me know. Thank you. *~Al*

Renaissance Fall 2022
Computer & Technology Classes

Register using Event Registration



New Intranet
Sid will present his personal approach to using the new Resident Intranet features. Early registrants will be sent an email asking for email responses containing questions about new Intranet matters they would like covered in the class. The class will then focus on those questions, first received, first covered. Please verify you have a good email address in the online Resident Directory.

Wednesday, September 21
10:00 am - 11:30 am
Cultural Center Education Room
Presenter: Sid Paskowitz, Spring Run resident

Gmail – 101
Gmail has a myriad of features and settings to make one become more productive. We will explore some of these. Specifically, we will explore various features of creating an email, searching emails, organizing emails as labels, auto adding an event and task from an email to calendar and shortcuts, adding and organizing contacts, and a few key features of the Gmail setting. The focus will be using Gmail on a computer and not on mobile devices.

Tuesday, October 18
1:30 pm – 2:30 pm
Cultural Center Education Room
Presenter: Jay Shah, North resident

Sandworm
Russian hackers penetrated Ukraine businesses, radio and TV stations, and government agencies, making them unusable by Ukrainians. Those hackers also released the most destructive malware in history. This happened in 2014. Today, Russian hackers are attacking again and Ukrainians hackers are fighting back, even into Russia. Come hear the story.

Monday, October 10
1:30 pm – 2:30 pm
Cultural Center Education Room
Presenter: Al Williams, Garden Apts resident

Understanding TiVo
TiVo is the digital recorder of choice. If you already have one, learn some of the advanced features such as skipping through the Guide or displaying only your favorite channels, options for repeat recordings, accessing premium services, and playing recorded programs 30% faster.

If you're just curious about how a TiVo could be helpful to you, then this is the chance to learn more about it. The class will demonstrate the basic features. You'll see the great program guide, how easy it is to record programs, replay dialog you may have missed, skip commercials, and always record a program when it is shown even if you're not at home. The handout is very useful and includes basic use, several intermediate and advanced features, basics of installation and setup, and some troubleshooting suggestions.

Friday, October 21
10:00 am – 11:30 am
Cultural Center Theater
Presenter: Tony Poulos, Spring Run resident

Chuck Smith is our 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 Chuck (csmithii@aol.com) to volunteer or to offer ideas on topics needed.

YouTube -101
What is One Billion? What is One Billion Hours per day? Yes, that is how much viewing is done on YouTube around the world. In this overview, we will show you what variety of videos people watch on YouTube that you may/may not know! How to view them comfortably, how to download (and edit) them and how to share the videos with others. We will briefly explain how to create your own video, upload, and share your videos with others. Though you can make money on YouTube, we will not explore how to do it in this session.

Wednesday October 26
1:30 pm – 2:30 pm
Cultural Center Education Room
Presenter: Jay Shah, North resident

Information Central
Sid will present an overview of the key features of Information Central, the Computer Club home page on the Resident Intranet. Early registrants will be sent an email asking for email responses containing questions about Information Central issues they would like covered in the class. The class will then focus on those questions, first received, first covered. Please verify you have a good email address in the online Resident Directory.

Monday, November 7
1:30 pm – 2:30 pm
Cultural Center Education Room
Presenter: Sid Paskowitz, Spring Run resident

Introduction to Podcasts
Some of us may recall being glued to the radio as youngsters, listening to shows like "The Lone Ranger," and even hearing the nightly news broadcasts with our parents. The good news is that your days of audio enchantment need not be over. If you like to learn and be entertained at the same time, podcasts may be for you. There are over two million podcasts available on almost every conceivable subject. Learn about technical aspects of how to find and listen to podcasts. Podcast technology is easy to use and most are free. We'll pull from this quickly growing area of technology to sample and recommend some wonderful podcasts representing a wide variety of genres and tastes.

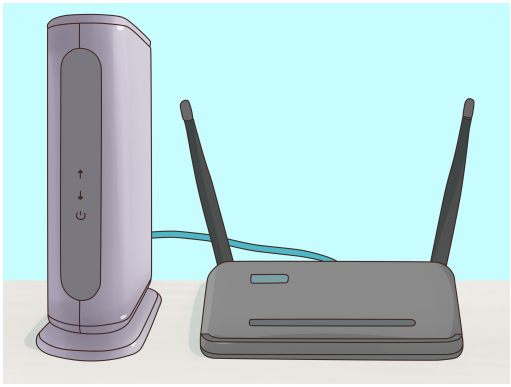
Tuesday, December 13
10:00 am – 11:00 am
Cultural Center Theater
Presenter: Dale Johnson, Spring Run resident

Just The Basics
This is a class where you can bring your own computer if possible or just come and listen! Lots of basic information, especially on Updates, router recycle, and Willow Valley Resident Intranet. Bring your own questions!

Tuesday, November 1
10:00 am – 11:00 am
Cultural Center Education Room
Presenter: Cathy Thorn, Gables resident

Managing Your Modem and Router
Computers, tablets, smartphones, TVs, and electronics of all types are dependent on connecting to the internet. How does your home network work? This class will provide modem, router, and network basics. You'll learn troubleshooting techniques you can use when your home network isn't working correctly.

Tuesday, November 22
10:00 am – 11:00 am
Cultural Center Education Room
Instructor: Tony Poulos, Spring Run resident



PC Housekeeping
Sid will present his personal approach to keeping his Windows 10 computer running smoothly. Early registrants will be sent an email asking for email responses containing questions about PC housekeeping matters they would like covered in the class. The class will then focus on those questions, first received, first covered. Please verify you have a good email address in the online Resident Directory.

Tuesday, December 14
1:30 pm - 2:30 pm
Cultural Center Education Room
Presenter: Sid Paskowitz, Spring Run resident

Privacy and Anonymity - Strategies

Discovery articles are written by Al Williams and are for those slightly familiar with the topic.

It is impossible to have complete privacy and anonymity and also be part of society. To obtain a driver's license you must give your name, address, date of birth; provide documents that verify your identity; and allow your picture to be taken. To obtain an accurate medical diagnosis, you submit your driver's license and insurance cards, provide detailed medical history, give blood for tests, and, if required, participate in diagnostic imaging.

Although your medical information is protected by HIPAA, your driver's license information may have already been sold. The Driver's Privacy Protection Act (DPPA) of 1994 allows the sale of driver's license information to a wide range of entities. Under the DPPA, some states allow the sale of name and address, and some also allow the sale of date of birth, ZIP code, phone number and email address.[1]

It is impossible to have complete privacy and anonymity and also be a part of society.

The Georgetown Law Center on Privacy & Technology issued the report *Data-Driven Deportation in the 21st Century* in May of 2022 describing how Immigration and Customs Enforcement (ICE) has collected driver's license information and also name and address information from local utilities that provide heat, water and electricity for years. The report states that ICE has used face recognition technology to search through the driver's license photographs of 32% of all adults in the U.S. ICE also has access to the driver's license data for 74% of adults and tracks the movements of cars of 70% of adults. The Center states that ICE has become a domestic surveillance agency.[2]

Advertisers also want your personal information so that they can target ads just for you. When you shop online, your purchases are recorded and become part of a dossier on you. Data brokers pull together data from retailers to create an even more extensive dossier on you. When you search for a product online and later see ads for that product or similar products it's because you're being tracked. Tracking makes it possible to present targeted ads.

Who you communicate with while using email, text messages, Facebook, Twitter, and other social media is recorded by those companies. This information helps to better understand who you are and how to better present ads to you. Data brokers collect this information as well.

Google collects your information. They say that they do not sell your information to advertisers but they monetize your data by building a profile for you with your interests and demographics like age and gender. They then let advertisers target those groups of people. Because of the profiling, the ads are a better match to you.[3]

Google also shares data with advertisers directly and asks them to bid on individual ads. The process is known as real-time bidding or RTB. The Electronic Frontier Foundation states "Real-time bidding is a convoluted, opaque system of data collection and sharing that enables profiling and surveillance by advertisers, data brokers, hedge funds, and ICE. It is at the center of everything that's wrong with privacy in tech."[4]

Google also has extensive records about who searched for what information. CNET reported that Google is giving data to police based on search keywords based on court documents. In the reported case, the search for the address of a residence that was done close in time to an arson incident was recorded by Google and later provided to police, leading to an arrest.[5]

Google also track phones. The New York Times reported that Google records people's locations worldwide. Investigators are searching that information to find suspects and witnesses near crimes. Google has tracking information that goes back for a decade.[6]

The US Congress passed the Cloud Act in 2018 which authorizes foreign governments to access the personal information of US citizens, or anyone

else, that is stored on servers owned by US companies. The purpose of the Cloud Act is to enable expedited access to support investigations of criminal activities. "…the Electronic Frontier Foundation, the American Civil Liberties Union, Amnesty International, and Human Rights Watch … argued that the bill stripped away Fourth Amendment rights against unreasonable searches and seizures, since the government could enter into data rights sharing agreements with foreign countries and bypass U.S. courts, and affected users would not have to be notified when such warrants were issued."[7]

You can take steps to protect your personal information.

And then there are criminals who want your money or personal information that they can use to obtain credit cards or open credit accounts. Sometimes your identity is sold. Twenty-six-year-old Madhumita Murgia has spoken about her experience when her identity was sold. I encourage you to listen to her story: https://www.youtube.com/watch?v=AU66C6HePfg.[8]

The situation is rather formidable. However, you can take steps to protect your personal information. You can work to put good and effective privacy laws in place. You can also ensure that you provide only absolutely needed personal information when requested. And you can ensure that you don't provide personal information in your emails or while using social media.

You may think that your personal information is already out there so why should you attempt to do anything about protecting it now. Your personal information is constantly aging. If you change your address, the old address is aged. If you change your cell phone carrier, the old carrier is aged. Everyone who wants your personal information will always want the latest. You should protect your personal information.

You may be concerned that protecting your personal information will draw attention to yourself. However, companies are aware of individual's desire for privacy and are encrypting your information in transit between our computing device and the company's web site (servers). Some companies are storing your information on their servers using encryption and some are not.[9] Unless you know the company is storing your information using encryption it is best to assume that they aren't.

If you use social media such as email, text messaging, Twitter, Instagram, and others, you should assume that your information is not protected by encryption unless you know that it is.

Moving forward, you should decide how you are going to care for your personal information. You should have a plan, even if it is a very basic plan. You will also need to select software and hardware to implement that plan. You'll need to follow good practices while following that plan. I'll discuss good practices, software and hardware in future articles.

Making Your Plan

The *Electronic Frontier Foundation* publishes a *Security Plan* for individuals under their *Surveillance Self-Defense* topic.[10] The plan asks five questions. I've reordered the questions for this article.

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?

Question 1

To answer the first question, what do you want to protect, I recommend that you consider the list from *Privacy Decrypted #7: What is PII?*.[11] I've added a few items to that list.

- Name, Social Security number, passport number, driver's license number, and taxpayer identification number
- Home address and email address
- Cell phone number
- Health information
- Financial records
- Photographs that identify you
- DNA
- Biometric data including fingerprints, retina scans, voice signatures, or facial geometry
- Date of birth
- Place of birth
- Mother's maiden name
- IP addresses
- Home phone number
- Race
- Religion
- Education achievement information
- Identification numbers for objects you own such as your car's Vehicle Identification Number
- Trade associations
- Professional associations
- Hobby associations

The list may not be complete for your needs. You should add any other personal information that you wish to protect.

Question 2

To answer the second question, who do you want to protect your information from, you must decide what person or organization might want your personal information. If you decide to make a list of who and why, it likely will become a large list and it will need to be continuously updated. The list approach isn't practical. But there is another way to answer this question.

In his book, *Understanding Privacy*, Daniel Solove discusses the concept of privacy in society. He says that although privacy is essential for societies, no one can reach a satisfying concept of privacy – what it is and what makes it unique and distinct. He therefore contends that a framework for understanding privacy must be grounded in the different kinds of activities that impinge upon privacy. He goes on to identify four categories of such activities and sixteen subcategories.[12] This framework covers more ways that your personal information might be taken when compared to the earlier examples.

- Information collection (surveillance and interrogation)
- Information processing (aggregation, identification, insecurity, secondary use, and exclusion)
- Information dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion)
- Invasion (intrusion and decisional interference)

> *"I've got nothing to hide and other misunderstandings of privacy."*
> *~Daniel Solove*

This category and subcategory approach helps to see the purposes for which your information might be wanted. It's then much easier to look at each subcategory and decide if that is an area of concern. If you are concerned about just one person or organization wanting it, that is sufficient to know that you need to protect your information. You don't need a complete list of who might want it.

There is a criticism of Solove's approach. He does not identify an underlying principle.[13] That means that new impingements on privacy must first be observed, recognized by consensus, and then categorized. The lack of a principle also means that consensus is required to determine that a possible privacy issue is not a privacy issue. Regardless, his categories and subcategories are extensive and useful and to date there is no need to extend the categories.

The term "concern" and similar words are common when describing why privacy is important, as you'll notice if you read the books listed in the *Privacy and Strategies – Drill Deeper* reference elsewhere in this newsletter. However, when discussing how to put privacy into practice the term "threat" is used instead. When putting privacy into practice, the perspective becomes: what could a malicious person or organization do?

Identifying threats and organizing them is known as threat modeling. When complete, the result is a threat model. Large organizations will devote significant resources to analyze threats and identify vulnerabilities in order to remediate those threats. However, for individuals at home, the threat model is easier to determine. A combination of good practices and selected hardware and software will be sufficient for most individuals.

Question 3

Only you can answer the third question, how bad are the consequences if your personal information is revealed? As you consider that question, I suggest that you keep in mind all the personal information items listed under Question 1.

Question 4

To answer the fourth question, how likely is it that I will need to protect it, I suggest that you think about all of the items as a group. That's because attacks on your privacy are aimed at obtaining as much personal information from you as possible.

Question 5

Only you can answer the fifth question, how much trouble am I willing to go through to prevent potential consequences. However, before deciding that you don't want to go to the trouble, I ask you to wait for future articles in which I will identity good practices, software and hardware that will minimize the effort needed to protect your personal information.

That concludes this article. Future articles will discuss good practices and hardware and software to meet privacy and anonymity needs.

Notes

[1] Motherboard: Tech by Vice: DMVs Are Selling Your Data to Private Investigators

[2] Georgetown Law Center on Privacy & Technology: American Dragnet: Data-Driven Deportation in the 21st Century

[3] DeleteMe: Does Google sell your personal information?

[4] Electronic Frontier Foundation: Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It

[5] CNET: Google is giving data to police based on search keywords, court docs show

[6] New York Times: Tracking Phones, Google Is a Dragnet for the Police

[7] CLOUD Act

[8] TEDxExeter: How data brokers stole my identity

[9] SecureCyber: The Internet is Going Dark; Here's Why

[10] Electronic Frontier Foundation: Your Security Plan

[11] Proton: Personal Data

[12] *Understanding Privacy* by Daniel J. Solove (Oxford University Press, 2008), multiple pages

[13] *Why Privacy Matters* by Neil Richards (Oxford University Press, 2022), page 19

Privacy and Anonymity - Drill Deeper

These resources explore the value and meaning of privacy and anonymity. They are some of the resources for the *Privacy and Anonymity* articles published in the July 2022 and September 2022 issues.

Privacy is Power - Why and How You Should Take Control of Your Data
Melville House - 2021

Carissa Veliz is an associate professor at the Faculty of Philosophy and the Institute for Ethics in AI, as well as a tutorial fellow at Hartford College at the University of Oxford. She is the editor of the *Oxford Handbook of Digital Ethics*.

Nothing to Hide – The False Tradeoff between Privacy and Security
Yale University Press - 2011

Daniel J. Solove is John Marshall Harlan Research Professor of Law, George Washington University Law School. An internationally known expert in privacy law, he is the author of several books, including *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* and *Understanding Privacy*.

TED Talks: Why privacy matters

Glenn Greenwald was an investigative journalist for *The Intercept*.

Teach Privacy: 10 Reasons Why Privacy Matters

See the Daniel J. Solove bio above.

Schneier: Privacy and Power

Bruce Schneier is the author of over a dozen books. He is a fellow at the *Berkman Klein Center for Internet & Society* at Harvard University; a Lecturer in Public Policy at the *Harvard Kennedy School*; a board member of the *Electronic Frontier Foundation* and *Access Now*; and an Advisory Board Member of the *Electronic Privacy Information Center* and *VerifiedVoting.org*.

Proton: Privacy Blog

A blog about privacy basics, privacy deep dives, and privacy news. Written by many authors for those unfamiliar with the topic.

Harvard Belford Center: Why Online Anonymity Matters

Afsaneh Rigot works under a pseudonym. Exposing her identity would threaten her family and herself due to the nature of her work and the countries she works in. This article was published by the *Harvest Kennedy School's Belfer Center for Science and International Affairs.*

LiveWorld: The Benefits of Online Anonymity

A post by Matthew Hammer for those unfamiliar with the topic.

Understanding Privacy | Harvard University Press 2008

See the Daniel J. Solove bio above.

Why Privacy Matters | Oxford University Press 2022

Neil Richards is one of the world's leading experts in privacy law, information law, and freedom of expression. He holds the Koch Distinguished Professorship at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine and Law. He is also an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, a Fellow at the Center for Democracy and Technology, and a consultant and expert in privacy cases. Richards serves on the board of the Future of Privacy Forum and is a member of the American Law Institute. He is the author of *Intellectual Privacy* (OUP).

Security News – September 2022

News for the home computer user to help you stay aware

Ars Technica: Why Lockdown mode from Apple is one of the coolest security ideas ever

Ars Technica: A wide range of routers are under attack by new, unusually sophisticated malware

Ars Technica: Discovery of new UEFI rootkit exposes an ugly truth: The attacks are invisible to us

Ars Technica: The Booming Underground Market for Bots That Steal Your 2FA Codes

Krebs on Security: Why Paper Receipts are Money at the Drive-Thru

Krebs on Security: KrebsOnSecurity in New Netflix Series on Cybercrime

Ars Technica: Google allowed sanctioned Russian ad company to harvest user data for months

Bleeping Computer: Hacker claims to have stolen data on 1 billion Chinese citizens

Ad Exchanger: T-Mobile Rebrands Its Ad Biz And Navigates The Perilous Line Between Programmatic And Privacy

Bleeping Computer: Google blocked dozens of domains used by hack-for-hire groups

Wired: 'Supercookies' Have Privacy Experts Sounding the Alarm

Wired: The Worst Hacks and Breaches of 2022 So Far

Ars Technica: Zero-day used to infect Chrome users could pose threat to Edge and Safari users, too

ZDnet: The next big security threat is staring us in the face. Tackling it is going to be tough.

Bleeping Computer: How China Hacked US Phone Networks

Wired: Here's Why You're Still Stuck in Robocall Hell

Wired: Russia Is Taking Over Ukraine's Internet

Bleeping Computer: US: Chinese govt hackers breached telcos to snoop on network traffic

NBC News: Russia says West risks 'direct military clash' over cyberattacks

Wired: Google Warns of New Spyware Targeting iOS and Android Users

The Hacker News: Researchers Warn of New OrBit Linux Malware That Hijacks Execution Flow – An Overview

Intezer: OrBit: New Undetected Linux Threat Uses Unique Hijack of Execution Flow – The Details

Intezer: Summary of Symbiote Research (A New, Nearly Impossible-to-Detect Linux Threat)

Intezer: Symbiote: A New, Nearly-Impossible-to-Detect Linux Threat

Krebs on Security: The Security Pros and Cons of Using Email Aliases

How-To Corner – September 2022

A collection of information that may be useful or interesting

How-To Geek: Getting Older? Here's How to Make Windows More Comfortable

How-T- Geek: How to Reset All Settings on iPhone

How-To Geek: How to Make Folders and Organize Apps on iPhone

How-To Geek: How to Clean the Dust Out Your Laptop

Schneier: When Security Locks You Out of Everything

Wired: How to Set a Maximum Limit on Your Phone's Volume

ProtonVPN: What is an IP Address?

How-To Geek: What to Do If You Drop Your Smartphone in the Ocean

Unredacted: Unredacted Issue 3 – A Magazine with Privacy, Security, and Open Source Intelligence News

Apple Insider: How to use Apple's ultra-secure Lockdown Mode and when you would want to

How To Geek: What's New in Windows 11's 22H2 Update: Top 10 New Features

Review Geek: Rufus Lets You Install Windows 11 Without a Microsoft Account

How-To Geek: This Tool Now Helps You Install Windows 11 on Unsupported PCs

How-To Geek: How to Enter the BIOS on Your Windows 11 PC

TEDx Reflections on Cybersecurity September

Cyber security for the human world
George Loukas | *All Things Connected*

.

How data brokers sold my identity
Madhumita Murgia | *All I Have Left is My Name*

.

Think Cyber – How to stay safe in an online world
May Brooks-Kempler | *Social Engineering Stings*

.

Your Human Firewall – The Answer to the Cyber Security Problem
Rob May | *It Takes a Village*

.

Cybersecurity every day
Jaya Baloo | *Stay Aware*

.

Internet of Things Security
Ken Munro | *Fix Yourself*

TERMINOLOGY

What is malware?

Malware is a general term for any software that will do harm to computers. What is it? This author explains:

What is malware?
https://protonvpn.com/blog/what-is-malware/

What's Happening

Windows Updates

In the past we have suggested waiting for a week or so after Microsoft released a new Windows update. My recent experience has been that problems residents are having with printing or other computer functions have been resolved by being proactive with Windows updates, including all optional updates. Even though an initial check for updates displays a message saying Windows is up to date, I have found that not to be the case. Not all updates are automatically installed and some won't install until the computer is restarted. My personal recommendation is to repeat checking for updates, including optional updates and restarts, until the computer confirms all the updates have been downloaded and installed. You might also want to click on this link to PC Housekeeping in Information Central. *~Sid*

Short Announcements/Alerts/Warnings

- Use Two-Factor Authentication (2FA) and Multiple Factor Authentication (MFA) when available.
- Have at least two browsers installed. Where one may not work with a specific website, another one will.
- Check Information Central for the most current information on Windows 11, including instructions for how to install.
- Microsoft will support Windows 10 through October 14, 2025.
- Update all software.
- While the Windows operating system is updating (usually on Tuesdays), your computer may be sluggish. Be patient!
- Information Central now includes links to videos from Computer Club meeting programs and classes.

Computer Device Support

#1 Try to get your own answers

We are often asked questions that can be quickly answered without needing to ask another person. If you know the key words in posing questions to another person, you probably know enough to use those words in a search engine where you could get the answer as a text display you can select and print, or a YouTube video you can watch.

#2 Personal Help with Computer/Device

We have developed a program for residents to **Get Help** with a wide range of daily issues, including computers and mobile devices. See page 1.

#3 Computer club support volunteers may come to your residence or may use **TeamViewer** or **Zoom**.

The Computer Club uses Zoom for video conferencing **but recommends against discussing private or personal information on it.**

Recommended Software

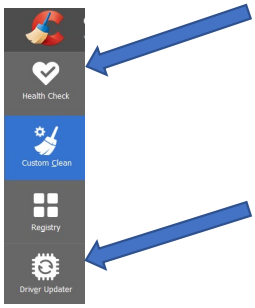
PC owners are reminded they will receive the best help if they use software that is familiar to other resident volunteers who provide technical assistance.

Recommended applications are **CCleaner**, **Malwarebytes**, **Defraggler** and **Windows Defender** (or **Windows Security Essentials**). We recognize there are alternatives; however, problems are more quickly diagnosed and repaired when the applications running on the PC are familiar to the helper.

Please use the Club's preferred Firefox, and limit using Internet Explorer, Edge or Chrome.

Action

CCleaner Issues. Some updates to CCleaner include **checked** boxes that allow the CCleaner update to install *Avast* or the CCleaner browser. Uncheck those boxes. We have found the *Avast* software to be a memory hog and a program that interferes with protections that Windows provides. Use CCleaner >Tools to uninstall Avast if Avast has been installed. We have limited experience or knowledge about CCleaner browser and, at this time, we are not recommending installing it.



The current version of CCleaner Free has two features options, Health Check and Driver Updater, that appear to be sales tools for the paid version of CCleaner rather than the basic CCleaner Free features. I don't use them.

Warnings

Exercise caution when **using Google or another search engine to locate customer service phone numbers of product manufacturers or businesses.** The Better Business Bureau recommends using the contact information from a product's equipment manual, or directly from the company's website after double-checking that the URL is correct, or finding contact information on your bill or in a confirmation email. It is too easy for a bogus website to be made to look like a legitimate company site and the web address of that website to be very similar to the legitimate company's name. Be especially suspicious when the address of the website as shown in the status display (usually in the bottom-left corner of the screen) or text bubble ends in ".UR" or ".RU" or something other than .COM, .ORG, .NET or .INFO which legitimate companies are more likely to have.

Fake Emails. Residents occasionally get an email from someone they don't usually hear from. They are almost always scams or contain malicious software. **Don't open them. Don't click on their links. Don't call the phone numbers they display.**

Malicious software. Google continues to find Android spyware in its app (application) store "Google Play." **That spyware has been there for years without being noticed**. Millions are potentially affected.

Caution!! When you are not using Alexa or Google Assistant, TURN THEM OFF by removing the power source! Protect yourself. While using them, be careful what you say.

If you have an Amazon device such as Alexa, it may have a feature called Sidewalk. That feature allows smart devices to connect to neighbors' Internet service and neighbors to connect to yours. If you have one of the Amazon smart devices, go into that device's application and look for **More** in the settings. If **Sidewalk** is listed as a setting, the Computer Club recommends the Sidewalk setting be turned off. See https://www.howtogeek.com/732351/what-is-amazon-sidewalk-and-should-you-disable-it/

Scams and Hacks

Hang Up
Disconnect
Shut Down
Unplug

Don't Open
Don't Click
Don't Call

No one who calls you, emails you or displays a message on your computer or device can tell you your computer or device is infected or running poorly. They have to have been given access. If you haven't given them access, you are being scammed. Don't give them access. **Hang up. Disconnect. Shut down. Unplug.** Do not respond to emails that say your account is missing information or that say they were not able to deliver a package with something you did not order. ***Be skeptical. Protect yourself***.

Several residents are asking for help when they see a message on their screen that tells them that they have been hacked or that claims to be from Microsoft. The message looks official. It says that their computer is locked (and it is), that they must not turn off their computer, and to call the phone number on the screen.

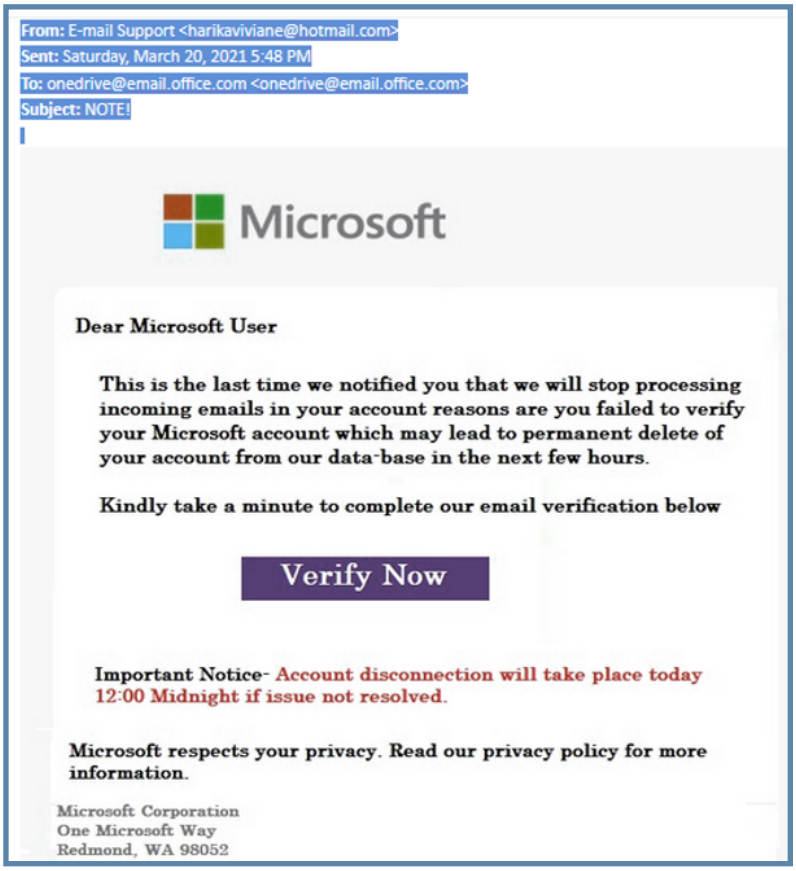
Do not call that number. It is a scam. If you do follow their instructions, they will download and install software on your computer that gives them access to your information. Instead, follow these steps to recover your computer.

If you do not use a password to access your computer:

1. Hold down the power button until the computer turns off. It may take several seconds.
2. Wait 10 seconds and restart your computer.
3. If the message reappears, hold down the power button again until the computer turns off.
4. Unplug the computer from the outlet and wait four hours. If you are using a laptop, remove the battery and wait for four hours. **NOTE**: MacBook owners should not attempt to remove their laptop battery. That should be done only by an authorized Apple technician.
5. Plug the computer in or if using a laptop, replace the battery.
6. Restart your computer.
7. If you still have the message, ask for help.

If you use a password to access your computer:

1. Hold down the power button until the computer turns off. It may take several seconds.
2. Wait 10 seconds and restart your computer.
3. Do not log into your computer.
4. Follow the appropriate instructions below
   A. PC Users: On the bottom right of your screen locate the Power icon. Select Restart.
   B. MacBook Users: On the bottom of your screen, click the Restart button.
5. When the login screen appears, log in.
6. The log in may take longer than usual.
7. If you still have the message, ask for help.
8. You may get help using the **Get Help** instructions on page 1 of this newsletter.



From: E-mail Support <harikaviviane@hotmail.com>
Sent: Saturday, March 20, 2021 5:48 PM
To: onedrive@email.office.com <onedrive@email.office.com>
Subject: NOTE!

Microsoft

Dear Microsoft User

This is the last time we notified you that we will stop processing incoming emails in your account reasons are you failed to verify your Microsoft account which may lead to permanent delete of your account from our data-base in the next few hours.

Kindly take a minute to complete our email verification below

Verify Now

Important Notice- Account disconnection will take place today 12:00 Midnight if issue not resolved.

Microsoft respects your privacy. Read our privacy policy for more information.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

This email was sent to one of our residents. It looks real; however, if you look closely, you can spot some things that indicate it is a scam.

1. the **From** address is **not** from Microsoft.
2. the **To** address is **not** to the person receiving the email.
3. the first line in the paragraph (**This is the last time we notified you**) is **not** good grammar.
4. there is no punctuation where there should be. The email states to read their privacy policy, but no link is provided.

If you get something like this, DON'T click on anything, just delete it!

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"

Technical Tips

Resident Copiers/ Printers. Contact your concierge for specific information on location and usage instructions.

The Computer Club recycling team has an inventory of computing devices available **FREE TO COMPUTER CLUB MEMBERS.**

WeTransfer.com— The service provides facilities to transfer (i.e., send or share) files that are too large to be sent as email attachments:

- No storage
- Send up to 2 GB
- Email transfers to up to 3 people
- Link transfers to unlimited people

The Computer Club recycling team has given away more than 480 computer systems to local community support organizations. Thank you.

The best way to deal with malware is: **Keep Devices Current**. Almost all modern electronic devices that are susceptible to malware (malicious software) provide facilities to update their software (applications) and firmware (code that tells hardware what to do). There are too many devices and versions to provide a single set of instructions for keeping devices current. Use Google or other search engines to get information on keeping devices current, or ask for help.

Spring Run Business Center on the 5th Floor of the Spring Run core building has a Windows 10 computer that can read SD cards and 3½ floppy disks. It also has an attached flatbed scanner that can scan documents and pictures, as well as convert scanned text in a document to a digital text file, using Optical Character Reader (OCR) software. If you bring your own flash drive, you can copy any of those files onto your flash drive and take them home for later use. Many of us have a stack of 3½ floppies we can't read.

Recuva software has been added to the Windows 10 computer to aid in recovering files on a damaged CD or DVD.

Inkjet Printers: Given up on your inkjet printer because you don't use it often enough and the ink dries and clogs the printer nozzles? This does not necessarily mean that you need a new printer. You can use the "clean" function on the printer to clear the nozzles and to clean the print head; be aware, however, this uses quite a bit of ink. If you prefer, look on the internet for alternate ways to unclog your printer.

Or, consider getting an inexpensive **laser** printer. Laser cartridges don't dry out and you can avoid leaving your residence to print documents on the Willow Valley printers.

RAM on new PCs. We recommend new PCs have at least 12 GB of RAM (Random Access Memory) for future needs.

Restore Point. There is a helpful article on how to remove software that you tried and no longer want on your computer. You have to set up your computer before hand. The article with its easy-to-follow instructions can be found on the Resident Intranet: Computer Club| Information Central or by clicking this link: Restore Point.

Backup Files: Please remember to periodically back up your important files to a flash drive, the cloud or external hard drive. Then, eject the drive and disconnect it from your computer so that those backed up files cannot be compromised. You never know when a computer might have a problem, and being able to put those saved files on a replacement computer can save a lot of time, money and headaches. Do not back up your files after your computer has been compromised. That can cause your backup files to be compromised as well. Get professional help if your computer has been compromised. Tony Poulos uses Backblaze for his backup service. Al Williams uses Amazon Web Services for his backup service. Gary Staton uses iDrive (not iCloud).

Microsoft and Windows General News

Microsoft Office

Microsoft is embracing subscription services for their products. Office 365 (now called Microsoft 365) has largely phased out its perpetual licensed counterpart - e.g. Office 2019 - by enticing users with a low up-front cost, continual updates, and additional perks utilizing Microsoft's cloud services.

Windows Updates

Although Microsoft had announced they were no longer providing updates to Windows 7 and Windows 8, they may provide updates for certain critical security updates.

During an update, the computer, screen, mouse, or keyboard may not responsive. Those conditions are not unusual during a Windows system update, some of which can take up to a couple of hours. The solution in many cases can be patience. If a computer is turned off during an update, problems can be created. Let your computer finish its update. Look for the light that shows activity on the hard drive. If it periodically flashes or stays lighted, your computer is probably working on installing an update. Let it finish and display a screen you recognize. If the computer continues to run overnight without restarting, press the power button until the computer turns off. Wait a couple of minutes and turn the computer back on.

If you still have concerns when your computer comes back under your control, run Malwarebytes and the full scan (after updates) using Windows Defender or Security Essentials to check for malware that may be on your computer.

Printer Problems with Windows 10 Updates

Several residents have reported printer problems after a Windows 10 update. One solution has been to connect and turn on the desired printer, go to *Printers and Scanners* in System Settings, add the desired printer if it doesn't show up in the list, select the desired printer as the default printer, then check to see if the problem has gone away. You could also use the printer troubleshooter.

Apple

Go to https://resident.willowvalley.org/cclub/gethelp.aspx to see lists of names of other residents who may be able to help you with Apple-related problems.

The Computer Recycle room, open Mondays 1:00 p.m. on the 5th Floor, Manor North J-Building, is accepting donations of Apple computers and devices. If, at the time of your donation, you leave a note with ALL (!!!) your passwords (login and Apple ID or passcode if an iPad or iPhone), your donation can be processed. With that critical information, the device can be totally erased and the latest operating system reloaded, making the unit available to Computer Club members and others. Without that critical password information, the unit will go to the county landfill drop-off point on Harrisburg Pike.

Support for all Apple devices is best found by any of the following listings. They are not listed in a particular order, although the first listing is the newest Apple Support service and may be the best available free service.

Download and use the Apple Support App on your iPad and iPhone for all Apple devices and services.
For Mac computers, go to https://support.apple.com/mac
Call Apple Support at 800-275-2273 for iPad, iMac or any MacBook devices.
Call Apple Support at 800-694-4766 for iPhones.
Go to the Apple Store at Park City Mall or contact https://support.apple.com/
Apple devices are not immune to scams or malware, especially if you use them to visit contaminated websites. Protect yourself.

Equipment Recycling Report

NOTE: The Computer Recycle Room will be open on Mondays only, from 1 pm to 4 pm. The Recycle Computer room 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 Recycle Room.

The Computer Club's recycling program refurbishes and recycles electronic devices. These refurbished devices are available free of charge to Computer Club Members and include Apple products, laptops, notebooks, monitors, printers, keyboards (including large print keys), cables, mice, power adapters, coaxial TV cables, and a variety of external devices including USB hubs that provide additional USB ports. Additional items are listed in the PC Recycling section of the most current Executive Committee (Board) Minutes on the Resident Intranet> Computer Club|Information Central or by clicking here.

Members should contact the Computer Center between 1-4 pm on Mondays if they have a specific request. Telephone: Call North Concierge Desk at 717 464 6000; ask for Ext. 2217 or dial directly on the Willow Valley telephone system.

Thanks to the team of volunteers, the Computer Club has donated over 400 devices to schools and charitable organizations in and around the Lancaster area. The Club recycles scrap through Full Circle Metal Recycling and the Lancaster County Solid Waste Management Authority.

TiVo Models

The current model is the Edge for Cable.

The TiVo Edge for Cable works with Campus TV. It will save up to 300 hours of HD programing. It has six tuners. Up to six programs can be recorded simultaneously. The cost for the unit is $399.99.

In addition to the unit, a TiVo service plan is required.
Monthly $14.99 with 1-year commitment, Annual $149.99, All-in (lifetime) $549.99.
Lifetime is the lifetime of the unit.

There are several sales during the year with significant savings. The units must be purchased directly from TiVo.

The regular price with annual service is $549.98.
The sales price with annual service is $349.98.

The regular price with lifetime service is $949.98.
The sales price with lifetime service is $549.98.

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.