Willow Valley Computer Club

May, 2025 | Newsletter | Volume 26, Issue 3

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:

Computer Club Leadership

- President: Al Williams
- Vice President: Dick Beidleman
- 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: Dick Beidleman
- Publicity: Bill Adams
- 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 our Fall, Winter, and Spring season concludes, I want to thank everyone who made it such a success. Our mission to provide effective computer education and practical support has been wonderfully met, thanks in large part to our dedicated educators and, notably, our incredible team of over 30 volunteers who tirelessly help residents navigate their computer challenges. Their selflessness and expertise are invaluable.

While our formal educational offerings will be less during the summer, the spirit of learning and assistance will continue, and we eagerly await the opportunity to further expand these beneficial programs in the upcoming year.

Al

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.

Computer Club Technology Center

NOTE: The Computer Club Technology Center (CCTC) is open on Mondays 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 original 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 are summarized below. The next two will be summarized in the July Newsletter.

➢ *Basic Cybersecurity for Personal Computers and Mobile Devices: Given on 2/11/25*

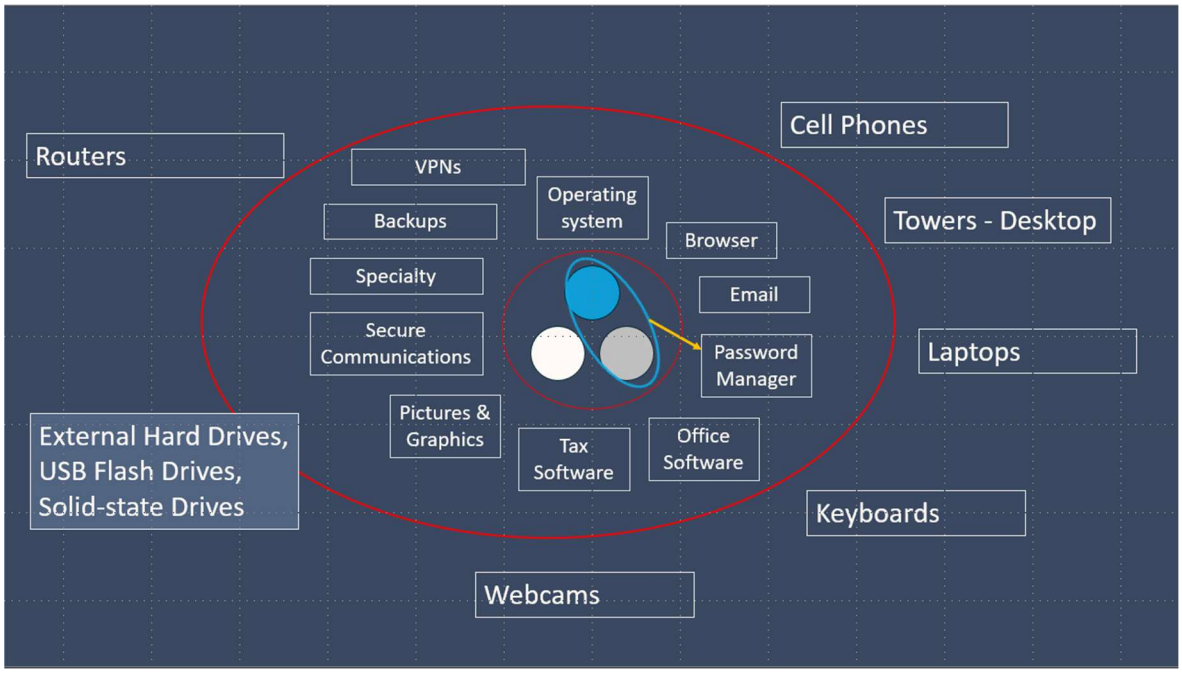
This topic deals with the issue that all computers and mobile devices - literally anything capable of connecting to the internet or cell phone network - are vulnerable to attack by cybercriminals in ways you may or may not be aware of. The only defense a user of these networks has is:

a. To understand the types of threats and how they occur
b. To learn about the available tools to help protect you against cybercrime
c. To learn how, when, and where to employ these tools.

It is an unfortunate fact of life in the internet and cell phone worlds that it is dangerous to ignore these threats because the consequences can be costly and emotionally upsetting.

No one, including WV residents, wants to spend time dealing with highly technical or even somewhat technical issues. We want to travel, attend concerts, dine out, call family and friends, maybe order something from Amazon, and eventually pay bills (OK, we don't want to). We want to do these things without thinking about the bad things that can happen. Unfortunately, that world no longer exists – not as long as there are people who can steal from you, too often without consequence.

The schematic below illustrates the modern world most of us deal with if we use computers, cell phones, and drive cars. At the center of this world is our information, which we store. Please think of this information as valued according to whether it's critical to protect (gold), important to protect (silver), and unimportant to protect (white). Surrounding this store of information are the various software tools we use to process the information. Outside this ring are the various hardware devices that store and/or access the software that processes this information.



Below are the Basic Cybersecurity suggestions residents should employ to protect their information. Space limitations mean we can only outline them. Detailed information is available at: WVCOMOUTERCLUB.ORG > Presentations > ***Basic Cybersecurity for Personal Computers and Mobile Devices.***

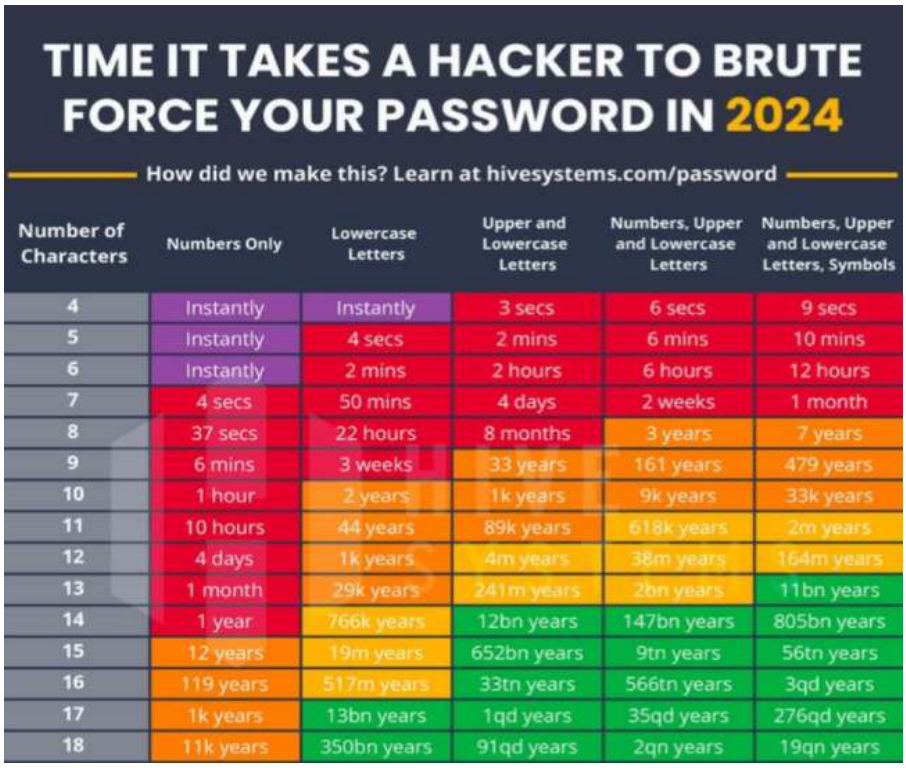
- **Vet technologies before using them**: buy only from reputable sources. Saving a few dollars by purchasing from third parties may prove costly in the long run.
- **Keep your device's operating system and apps up to date**. Tech companies frequently find flaws and improve their products. Updates fix the flaws and help increase your protection.
- **Ensure Operating Systems' Antivirus and Malware Protections are active: These tools are your first line of defense. Some are free, and others are modestly priced**. Paid products usually offer better support.
- **Avoid hardware with known vulnerabilities:** Average users may be unaware of such issues. Before buying, it's best to consult a WV Computer Club Technology Center person for advice.
- **Protect the physical security of your digital devices:** Take care of your phones and computers, especially when travelling. Please don't leave them unattended in public spaces. Back up important data on another device or external hard drive and store it in a safe place, such as a safe deposit box.
- **Implement User Account Control to protect your computer:** The more you use online websites, the more control (protection) you need, especially with financial websites. Use a password manager and implement multifactor authorization (MFA) when you can. Your password is the first factor, but you get additional protection by having codes you will only know sent to alternate devices and/or email accounts that you can access only. Top password managers are usually available for modest costs.

- **Manage application permissions for privacy and security:** Only install apps you need; delete those you don't use. When apps are installed, be careful when granting access to those apps.

➢ ***Protecting your accounts from compromise: Given on 2/25/25.***

Cybercriminals are constantly looking for ways to steal information from people. They often do so by finding the path of least resistance. In other words, they attack accounts of those who naively think that cybercrime happens to others, or perhaps believe that they don't have to employ even the most basic way to protect their data – strong account passwords. Actions to take to prevent your account from being compromised are summarized below.

- **Formulate Strong Passwords and PIN Codes.** Using strong passwords is a simple and effective means of protecting your data. These are long strings of text, symbols, and numbers. The longer the string, the better you are protected. The table below from Hive Systems tells you all you need to know about what password strength means as a way to deter cybercriminals:



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

The bottom line: the longer, the more complex the password, the harder it is to discover. Most people cannot remember a password longer than 8 to 10 characters, or perhaps create a longer password that is easy to remember (but maybe easy to guess). Moreover, many people have several accounts they access, which requires more passwords, or the temptation to use the same password for many accounts. The standard way to remember passwords is to write them down. Unfortunately, papers can be misplaced or lost. Furthermore, carrying a page of passwords with you if you travel is unwise because a list can be lost or stolen. In our current era, the only sensible approach is to use a password manager.

- **Use a Password Manager to Create and "Remember" Strong Passwords.** Some excellent password managers are available today. Some are free, and some require a (usually) modest annual fee to use. A significant difference between free and paid is the amount of support available should you need it.
  While it's true that we all want things for free, a key thing to consider is this: What is the value of paying what amounts to a few cents per day vs. the weeks, months, or longer it takes to recover from the cost of losing valuable information and/or money to cyber criminals?
  The password manager that the Computer Club recommends is Bit Warden (free or paid). 1Password is another good password manager. Here are the key requirements of a password manager:
  - Encrypted, so that only the user can see the data
  - Capable of generating and storing very long password strings
  - It seamlessly runs on multiple platforms: computers, cell phones, tablets, and smart watches. The main point is that you generate a password on one platform, and it's populated on all the other platforms where you have it installed.

  Finally, even if you have a password manager, as a precaution, it is a good idea to create an exported and encrypted file that is a copy of the password manager's contents. A paper backup should be used as a last resort and located where only you have access, such as a bank safe deposit box or home security safe.

- **A strong password isn't enough; use multifactor authentication (MFA).** In the early days of the internet, it was enough to have a simple password. The evolution of the internet has brought more valuable, helpful, and engaging websites for users and more ways for them to become victims. Unfortunately, even strong passwords are not enough because cybercriminals can sometimes get around even the strongest defenses. Websites like online banks are increasingly offering additional ways to protect users from cybercrime. One of these is MFA, an additional way for a website to ensure you are who you say you are. Examples of MFA include:
  - After entering a password at login, you must have a code sent to a device or alternate account, such as a cell phone or an email address that you have access to. This code exists for only a few minutes, and you must enter it into the website before you are given access.
  - After logging into a site, you must identify images or solve a puzzle – something a program planted on a website or your computer – a "bot" – could not easily do.
  - Activate using Face ID, in addition to your password.
- **Passkeys are a Good Thing.** From PC Magazine: A passkey is a way to log in to applications and websites without a username and password combination. It's a pair of cryptography keys generated by your device. Apps or websites store your unique public key. Your private key is only stored on your device. After your device authenticates your identity, the two keys combine to grant you access to your account. Usually, the device, or software generating the passkeys, uses a biometric authentication tool, such as FaceID or TouchID, to validate your identity. If a password manager is the passkey storage, you can log in to an app using a strong master password instead of biometric authentication. Passkeys are unique to each app or website and stored in a password manager's vault or your device's keychain (Apple's password manager). Passkeys in password managers can also sync across devices, making them a convenient choice.

Unfortunately, even Passkeys can be hacked by cybercriminals because they can exploit security holes in weak websites. Currently, passkeys are being implemented, and they are sometimes not easy to use. However, you should use passkeys as much as possible.

- **Email Aliases are also a Good Thing.** An alias is a secondary email address linked to your primary email account, allowing you to send and receive emails without creating a new account. This helps organize your emails and can be used for different purposes, like managing work and personal communications. A key aspect of aliases is that they can shield your main account from unwanted emails, like spam. The options for creating an alias email address vary; some good tools can help you create an alias. A valuable tool for creating aliases is SIMPLE LOGIN, available in a free and a paid version.

- **Some Browser Extensions are a Bad Thing.** Browser extensions are invoked when the browser is launched. They add features to the browser that are not ordinarily available, making it easier to access and use websites. However, cybercriminals can install malicious extensions. These extensions will capture your usernames and passwords. You should review the list of extensions in your browser periodically to determine if an extension should be removed.

COMPUTER CLUB TECHNOLOGY CENTER BI-MONTHLY REPORT

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

March – April 2025 Activity
North "J" 5th floor Technology Center
Hours – Monday 10am – 4pm (sometimes 9:30am – 5pm)

- **Center Open days – 9**
- **Active volunteer hours in CCTC – approximately 304**
- **Active WVCC volunteer hours outside CCTC – unknown**
- **Active current CCTC volunteers – 7 technical; 8 administrative**
- **Resident interactions at the CCTC**
- **Total Visits to CCTC – 118**
  - ✓ Apple issues – 16
  - ✓ Windows issues – 32
  - ✓ Printer Issues – 3
  - ✓ Phone/Miscellaneous – 16
  - ✓ Donations – 32
  - ✓ Product Requests – 19
- **Known phone calls from/to residents – approximately 20**
- **Known visits to resident's locations – approximately 15**
- **Printer setup and connectivity issues**
- **Connectivity issues, including TiVo and other log-on security issues**

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.

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"