



# THE WYSIWYG



May 2020

Volume 32 Issue 5

**STERLING HEIGHTS COMPUTER CLUB**

PO Box 385

Sterling Heights, Michigan 48311-0385

**MAIN MEETING: TUESDAY MAY 5  
7:00 PM**

Same day/time as usual

Location: Your house,  
Video conference

\* \* \* \* \*

Farewell, Baker College.  
We enjoyed our stay!

**IN THIS ISSUE:**

About SHCC	2
President's Pen // Your Data is Shared and Sold	3
Windows 10's Bugs Are Teaching the Importance of Backups	4
Flush the DNS Cache in Windows	5
A Recent Scam Experience	6
Why Is My Computer So Slow?	7
File Extensions — Helpful or Not	8
How To — Keyboard Fix	9
Windows Free Snip and Sketch Tool is New and Replacing the Old	10
Wi-Fi Security — Which One: WEP, WPA, or WPA2?	11
Are Identity Theft Protection Services Worth It?	12
Use This Hidden Keyboard Combo to Fix Your Frozen Computer	13
Web Page Reviews	13 & 14

**This Month's Main Meeting Topic:**

**“Tune Up Your Windows PC”  
will be presented online by  
APCUG Speakers Bureau member  
Jere Minich**

\* \* \* \* \*

Due to the prevailing concerns for public health and limitations as mandated by the MI State Government, a traditional May meeting at Baker College cannot take place.

Instead, this online meeting is scheduled for May. Our club President sent an email message to you on April 24 with meeting access details. If you did not receive his message, contact him or one of the other Officers for the meeting details. Their contact email addresses are on page 2.

*Hope to 'see' you there!*

Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding whether to become a member or not. July and August don't count since there is no main meeting in those months. Membership includes admission to all SHCC functions and the newsletter. Membership is open to anyone. It is not limited to the residents of Sterling Heights.

**DUES: \$30/YEAR**

**CLUB ADDRESS:** PO Box 385, Sterling Heights, MI 48311-0385  
**CLUB E-MAIL ADDRESS:** [Info@SterlingHeightsComputerClub.org](mailto:Info@SterlingHeightsComputerClub.org)  
**CLUB WEB PAGE:** <http://www.SterlingHeightsComputerClub.org>

## 2020 SHCC Officers – Thanks to all!!!

<b>President</b>	<b>Don VanSyckel</b>	President@SterlingHeightsComputerClub.org
<b>Vice President</b>	<b>Mike Bader</b>	VP@SterlingHeightsComputerClub.org
<b>Secretary</b>	<b>Martee Held</b>	Secretary@SterlingHeightsComputerClub.org
<b>Treasurer</b>	<b>Bernie DeFazio</b>	Treasurer@SterlingHeightsComputerClub.org

### Resource People

Firefox	Don VanSyckel
General Computer Questions	Jack Vander- Schrier
Hardware	(open)
MS Publisher	(open)
MS Word	Rick Schummer
Spreadsheets	Rick Schummer

### SHCC Coordinators

Associate Editor	Rick Schummer
Door prizes	Don VanSyckel
Greeter for visitors	Jim Waldrop
Newsletter Publisher/Editor	Paul Baecker
Program Coordinator	Mike Bader
Publicity	Patrick Little
Publicity	Phil Reynaud
Welcome & check-in desk	Jim Waldrop
Web Site Admin	Don VanSyckel
Web Watch column	Paul Baecker

### Contact Information

(Use the appropriate e-address for your questions/comments.)

Mike Bader	586-447-6683	programs@sterlingheightscomputerclub.org
Paul Baecker		newsletter@sterlingheightscomputerclub.org webwatch@sterlingheightscomputerclub.org
Patrick Little	586-264-1497	publicity@sterlingheightscomputerclub.org
Phil Reynaud	586-212-2848	publicity@sterlingheightscomputerclub.org
Rick Schummer		assoc-ed@sterlingheightscomputerclub.org
Don VanSyckel	586-731-9232	doorprizes@sterlingheightscomputerclub.org webmaster@sterlingheightscomputerclub.org
James Waldrop	586-731-6481	greeter@sterlingheightscomputerclub.org check-in@sterlingheightscomputerclub.org

### Club Dues Amounts

The club dues were increased to \$30 per year at the November 2018 meeting.

This includes a digital version of the newsletter sent monthly, except for July and August, when the club does not meet.

A paper version of the newsletter is available in place of the digital newsletter, for an additional \$31 per year. (increased at March 2019 meeting)

Associate memberships, for a second member of a household, remain at an additional \$15 per year.

### Four-Month Meeting Schedule

**JUNE 2020**  
 2 - SHCC Main Meeting  
 14 - SEMCO meeting

**AUGUST 2020**  
 SHCC — NO Meeting  
 9 - SEMCO meeting

**JULY 2020**  
 SHCC — NO Meeting  
 12 - SEMCO meeting

**SEPTEMBER 2020**  
 1 - SHCC Main Meeting  
 13 - SEMCO meeting

Newsletter submissions are due 10 days before the club meeting, but the earlier the better. They should be sent to : [newsletter@SterlingHeightsComputerClub.org](mailto:newsletter@SterlingHeightsComputerClub.org)

© Unless stated otherwise, all materials contained in this newsletter are copyrighted by the Sterling Heights Computer Club. License is hereby granted to other clubs (non-profit) to reprint with credit.

## The President's Pen

by Don VanSyckel



Last month's meeting was canceled due not being able to respond to the pandemic shelter-in-place meeting restrictions. To date, we have not heard when restrictions are going to be lifted, just that restrictions will probably be lifted in phases. Because of this uncertainty, this month's meeting will be held as a virtual meeting. Our presenter will be one of the APCUG speakers bureau presenters.

Reminder: APCUG is the Association of Computer User Groups, in short, a club of clubs that SHCC belongs to. Many of you have "attended" one or more of the APCUG quarter virtual seminars held on Saturdays. The APCUG speakers bureau uses ZOOM to conduct their virtual seminars and remote presentations. I realize there have been various articles in the press and trade publications about ZOOM, but you have to go with the flow when using someone else's free service.

I remind you from previous articles that I've cut the cord a few months back. Well, with more time on my hands, I can't even get close to running out of free content to stream. I'll say up front that the current movies and shows are not available for free. Having said that I'm finding more content than I can consume. There are many movies that I never saw when they were new but they are still enjoyable to watch even though they are a few years old. Granted most of the free content comes with commercials but I've been watching TV with commercials for so long that I can tune out a few ads. Also, if you aren't familiar with streaming services, some convenient features are pause and continue later or the next day, fast forward through scenes that are moving a little too slowly, rewind that some of you call instant-replay, and stop on one device and pick up on another device.

If you do decide to use a streaming service such as [Tubi](#), [Vudu](#), [Crackle](#), [Popcornflix](#), and others, look for the "want list" or "queue". Many have long lists of available content that I don't want to navigate over and over. I go through the list once and add the items I have interest in to my "want list" and then view items from there. By the time I get through the "want list" the service has made a new group of items available so I go through the list once again.

If you have to have certain content, the major networks, Hallmark Movie Channel, History Channel, and others offer monthly subscriptions generally for \$5 to \$10 a month. These generally offer current content as well as previous shows. These services have a limit on how many devices can use the service simultaneously, so check before you sign up. They all state the limit but it's difficult to find it sometimes.

Don't forget the library, when it reopens in a month or so, they have a lot of content from Hallmark Movie Channel, History Channel, and others. {Ed. note: Of course, different libraries offer different audio and video streaming options. Go to YOUR library's web site to see what educational and entertainment options exist for your library card. Don't have a library card? Some libraries are creating patron accounts in absentia during the shutdown period. Just call your local library to find out.}

There are also services like Sling TV that offer both local channels and premium channels. I almost signed up for Sling TV, but the one device limit made this too expensive for two TVs. Then there's Amazon Prime which costs \$119/year, but you

get free shipping of stuff you purchase. On the other hand, I don't have Prime and get free shipping anyway.

I haven't even touched on the \$50 high definition antenna I bought and set up in the attic. All the local channels are crisp and clear.

The meeting info email was sent to you on April 24 (see note on page 1). If you don't get an occasional email from SHCC, send Martee an email to keep your email address up-to-date: [Secretary@SterlingHeightsComputerClub.org](mailto:Secretary@SterlingHeightsComputerClub.org)



## Your Data is Shared and Sold

News and/or Opinion from Paul Baecker

A link to an article titled "Your data is shared and sold...What can you do about it?" (see page 13) discusses how our privacy is under attack daily, whether we use the Internet or not. A few key comments from the article:

*Some consumers are often not aware all of the tracking and analysis is going on and thus don't do anything about it. One way they are lulled into complacency is by the presence of a privacy policy on a website, app or mobile service. But these policies are an exercise in "obfuscation" because most people don't read them or don't understand them. Up to 73% of American adults incorrectly believe that the existence of a privacy policy means a website cannot share their data with other parties without their permission.*

*Even the label itself — privacy policy — is misleading. It's a deceptive label because most people misunderstand it. Instead of protecting the consumer's privacy, the purpose of a privacy policy is to protect the company. And within the policy itself, companies typically use language that is often very broad to the point that it will allow them to do a lot of things that you don't necessarily understand unless you can read between the lines.*

*Companies don't make it easy for consumers to find out exactly how their data is being used. Corporations use four common strategies whose goal is to distract the consumer from questioning data privacy practices.*

*These four tactics — placation, diversion, misnaming and using jargon — contribute to a feeling of resignation among consumers. Since they can't fight this data collection and tracking, they might as well give up.*

But what steps can you take to reduce the level that you are tracked while you are surfing the Internet?

- \* Add a free ad-blocker to your web browser to reduce clicking temptations. (My current choice is "Ublock Origin".)
- \* Add a free tracker-killer to your web browser (*trackers* are different from *cookies*). (My current choice is "Ghostery".)
- \* Use a free tool to delete cookies from your browser DAILY. (My current choice is "Ccleaner".)
- \* Use a web browser and search engine that minimize invasion into your privacy. (My current choices are "Firefox" and "DuckDuckGo".)
- \* Subscribe to a paid (not free!) VPN service to make you and your IP address as anonymous on the web as possible. (My current choice is "PIA -- Private Internet Access".)



## Windows 10's Bugs Are Teaching the Importance of Backups

By Chris Hoffman  
[www.howtogeek.com](http://www.howtogeek.com)

Windows 10 has now had multiple automatic updates that accidentally deleted people's files. Buggy updates have caused problems with hardware drivers, too. Microsoft highlights the importance of having good backups and being prepared for anything.

### Buggy Updates Aren't the Only Danger

Okay, we're giving Windows 10 a hard time here. But it's far from the only thing that can delete your files. For example:

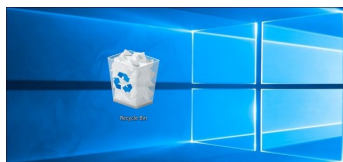
- The solid-state drive, or hard disk in your computer, could die, taking your files with it. The S.M.A.R.T. system is designed to provide some warnings about dying hard drives, but it doesn't always work.
- *Ransomware* or other malware could infect your system and encrypt, or erase, your files. Even if you're careful, you could be compromised through a zero-day bug in an application you use.
- Another application on your system could have a bug that accidentally deletes your files or corrupts your file system. (Remember that time when Google Chrome's updater corrupted the file systems on some Macs?)
- A freak power surge, or lightning strike, could destroy your computer's hardware.
- You might accidentally overwrite an important file.
- A thief could steal your laptop.
- Your home could catch on fire, destroying your desktop PC.

These potential problems go on and on. But, despite that, many people don't regularly back up their files. Everyone should.

Let's highlight a risk that seems extra scary to many people: Windows Update could automatically delete your files. An automatic update could just arrive one day and you may find your files gone or your computer unbootable.

### Yes, Windows Update Has Caused Problems

Windows 10 updates have deleted people's files before. They might do it again! Even aside from file



-deletion issues, update bugs could potentially corrupt your operating system until you [reinstall Windows 10](#). Let's take a quick look:

- [Windows 10's botched October 2018 Update](#) was pulled because it deleted people's files in some situations. For example, if you had ever moved your Documents folder at C:\Users\Name\Documents to another directory like D:\Documents, this update automatically deleted any files in the original folder location. Even if you had a folder packed full of files, Windows 10 just deleted it without asking.
- [A buggy security update released in February 2020](#) also deleted some people's files. Most affected people had their files vanish to another folder on their hard drive and could hunt them down, but some people report their files were gone for good.
- Buggy updates have caused bugs ranging from black screens at boot and broken mapped network drives. They have even prevented people from changing their default applications. Microsoft is testing their updates more lately, so things are looking up overall.
- Automatic hardware driver updates have broken everything from sound drivers to external media devices. They've even bricked some peripherals. Microsoft is trying to improve hardware driver updates, but they've been a problem on Windows 10.
- Windows 10 updates sometimes [delete people's programs without asking](#), too.

Do you really want all your files sitting on a Windows 10 computer, one buggy update away from vanishing? Of course not. Even if Windows 10 had a spotless track record of perfect updates, you still shouldn't keep a single copy of your files in one place.

Windows 10's history of update bugs should give you extra motivation to back up your important files.

Backups make it easy to recover from a catastrophic problem caused by update bugs, hardware failures, or anything else. Just reinstall Windows (or get a new PC), restore your files, and you're good to go.

### Backups Can Be Easy

Backups don't have to be complicated or hard. Here are some easy ways to [get started backing up your computer](#):

- [Use Windows 10's built-in File History feature](#). All you need is an external hard drive that plugs in via USB. Regularly connect the drive to back up your files. (You probably don't want to leave the external drive plugged in all the time. If you do, ransomware or other

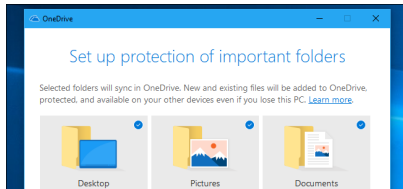
malware could attack your backup drive.)

- **Back up online.** Online backup services give you a chunk of online storage along with a desktop program that backs up your files. It will run in the background on your PC, automatically backing up your files to the online storage location. You won't even have to think about it. We recommend [Backblaze](#), which costs \$60 per year, or \$6 per month, and offers unlimited storage.

For best results, combine both options. You'll get local backups so you can quickly restore your backed up files if you ever have a problem. You'll also have ["offsite backups,"](#) which you can access if the worst happens and something (like a fire) takes out your computer and local backup drive.

### Cloud File-Syncing Services Can Help, Too

You can also use a cloud file-syncing service like Google Drive, Microsoft OneDrive, Dropbox, or Apple iCloud Drive, and store your important files there.



[These aren't technically "backups" in the usual sense.](#) Changes synchronize instantly, you only have so much space, and you can't just quickly restore all your files to the state they were in at a certain point in time.

However, keeping your critical files easily accessible in a cloud-storage service is better than just leaving them on one device. They'll be accessible to you even if something happens to your computer. That's why Microsoft is pushing [OneDrive Folder Protection](#) to "protect" your files if everything happens to your PC.

Are you worried about securing the files you're storing in a cloud storage service? Microsoft now offers [an encrypted "Personal Vault" in OneDrive](#), providing additional protection for sensitive files. Some other online backup services have similar options. For example, Backblaze lets you set a "private encryption key" to secure your backups. However, if you lose the key, you'll lose access to your backed up files.

### Preparing to Recover From Update Problems

Beyond backing up your files, it's a good idea to [ensure System Restore is enabled on Windows 10](#). This feature makes it easy to ["roll back" your system to a known-good state](#), and it can help if Windows 10 installs a buggy hardware driver update or operating system patch.

You should also consider [making a Recovery Drive or System Repair Disc](#), which will let you troubleshoot

problems if your PC ever becomes unbootable. You may also be able to [access Windows 10's Startup Repair options](#) without any recovery media, even if Windows 10 won't boot normally.

If the worst happens, however, you can always [create Windows 10 installation media](#) on any computer and use it to reinstall Windows 10 on your PC. You won't even have to enter a [product key](#) on modern PCs. If your PC came with Windows 10, the key is likely embedded in its [UEFI firmware](#). If you upgraded to Windows 10 from Windows 7 or 8, you likely have a ["digital license"](#) that will automatically activate when you install Windows 10 once again.

*This article is republished, with permission, from the How-To Geek web site.*



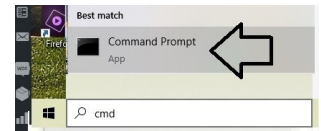
## Flush the DNS Cache in Windows

by Cyn Mackley

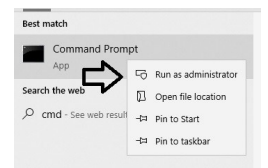
<https://cynmackley.com/category/cyns-tech-tips/>

If you're having issues with a web page just not loading right, I may have a fix for you. Especially if that page seems to load without any issue for other people.

Try flushing the DNS cache. Start by typing **CMD** in your search box.

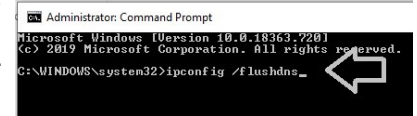


Right-click on the result and choose **Run as Administrator**. Windows will then ask for permission to make changes to the computer.

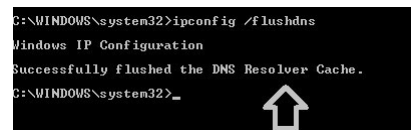


Type **ipconfig /flushdns**

Note that there is a space before the slash. Then press Enter.



If you're successful, you'll see **'Successfully flushed the DNS Resolver Cache.'** If it doesn't



say that, try typing again. Make sure you have that space before the slash.

*This article is republished, with permission, from the Cyn Mackley's Tech Tips web site.*



## A Recent Scam Experience

By Jeff Wilkinson, President  
Sun City Summerlin Computer Club, NV  
The Gigabyte Gazette [www.scscclb.com](http://www.scscclb.com)  
Clearmeadows11@gmail.com

Recently I received the "Social Security" scam call, the recorded message informing me that I should call an 800 number because my account was about to be suspended. I decided to play along and see what the suspected scam pitch was, since I was 99.99% sure that Social Security doesn't call you.

I called the 800 number, exclaimed my surprise that there was a problem and breathlessly asked what the problem was. The responder, "Officer Ronald Smith" explained, in an almost unintelligible accent, that he was a senior investigator and I should get a pencil and paper and write down his name and badge number, which he proceeded to give me. He then went on to outline the "problem" which included seven bank accounts opened under my social security number. He said the accounts had been used for money laundering and an investigation was underway with an arrest warrant about to be issued. In addition, there were multiple credit cards also under my social security number which had been linked to illegal activity.

"Officer Smith" then asked if these were my accounts. Upon my answering No, he explained he needed to know how many bank accounts and their approximate balance and how many credit cards I had and their credit limits. I responded with fictitious information of course. He advised me that this conversation was being recorded and I was repeatedly told to listen to his instructions very carefully. When I told him in a frightened, exasperated voice that the accounts he described were not mine, he wanted the local police department phone number so he could call to see if we could clarify some additional information. I gave him a fake phone number and he put me on hold; he came back a short time later and said that the number I gave him was incorrect!

"Officer Smith" then told me I could get the number from the yellow pages or Google and said he would wait while I looked it up. When I asked why *he* didn't have it, he exclaimed he did but was not allowed to give it to me. I looked up the number in the city I had claimed to live in and gave it to him; he again put me on hold and returned a couple of minutes later. He said he had a senior investigator on his other line, and she would be calling me. I was to put him on hold when she called.

Then my phone rang! The call was from the number I had provided which was the number of the Palo Alto, CA police department! "Officer Smith" told me to put him on hold and to add the new caller to the conversation.

Throughout this entire 22-minute ordeal he had not yet asked for any money or access to my computer. I was tempted to continue the charade, but the language barrier became intolerable along with the level of minutia, so I ended the calls. Almost immediately my phone began ringing from an unknown 800 number, over and over until I blocked the number. I believe the ploy was to obtain my information such as date of birth, address and social security number so they could steal my identity.

Although I didn't get far enough to determine the full scam, I was very surprised that they added so much credibility by calling me back and "spoofing" (faking the Caller ID) of the actual police department number I had provided and they had checked!! As we know, spoofing a phone number occurs often on junk and scam calls. This specific trick could cause a reluctant mark to falsely think they were maybe being too cautious. The scammer may attempt to retrieve your date of birth, name, address and partial social security number by asking throughout the conversation for you to verify the information. With those items, it is possible to initiate a change of address and phone number with Social Security and then redirect your direct deposit to a different bank.

Having repaired two cases of scammers gaining access to computers that week, one which was able to gain bank information and withdraw a four-figure sum of money from a retiree, I was interested in experiencing the actual pitch. It can't be stressed enough that allowing remote access to your computer from random phone calls, emails or web page screens is to be avoided. Also do not release any personal information to unknown callers no matter how official they attempt to sound. With so much information available in the public domain, many times only a small amount of additional information is needed to initiate an identity theft.

***This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.***



## Change of Meeting Venue

As you are probably aware by now, SHCC meetings at Baker College have ended. Starting in June 2020 the club will start to meet at the location below. You will be reminded via email late in May and in the June WYSIWYG. Be sure that the club has your current email address. Contact the Secretary if it needs updating.

**St. Thomas Lutheran Church  
8771 East 15 Mile Road  
Sterling Heights, MI**

**North side of 15 Mile  
about a third of a mile east of Van Dyke**

## Why Is My Computer So Slow?

By David Kretchmar, Computer Technician,  
Sun City Summerlin Computer Club  
Gigabyte Gazette      www.scscclab.com  
dkretch@gmail.com

There are plenty of computers being used that are performing much more slowly than they should. One of the quickest ways to turn a fast, new computer into a slow system crippled by malware is to start downloading what you think is good software from the wrong sites, or by downloading the wrong software from what appears to be the right site.

Newer computers being slowed by unwanted programs is a bother, but the damage done by PUPs (Potentially Unwanted Programs) can be much more serious; PUPs can be responsible for programs that lock up your system and make it impossible to access any of your files, or otherwise ruin your system.

Every time you download anything from the Internet you first issue permissions that enable the opening of a conduit between the Internet and your computer. The series of complex events is mostly invisible to you, except for your clicking on that virtual button that starts the whole process.

Bing and Google searches often can take you where you don't want to go. When searching for popular software, sponsored search results (which result in unwanted programs) often appear at the top of the search results page, along with links from the actual software source sites. Often those ad links try to install software on your computer that you do not want. It could be anything; it could be a fake driver update program or a scam system cleaning program. Note that my Bing search for VLC media player (left) first showed 4 sites NOT associated with VLC – places that have a high potential for providing bad software.

### Testing Misleading Advertisement Links

How bad is it? To find out, I installed a fresh Windows 10, plus all Windows updates, on a freshly formatted hard drive. I downloaded and installed the free version of Avast! Antivirus software that brought a hitchhiker of its own - Google Chrome. OK, I wanted Chrome, but not every user would so I considered this an invasive act by

a program I downloaded for protection.

I used Edge, Firefox, and Google Chrome and started using Google and Bing search engines to start searching for popular free programs. The programs I sought are often the first programs that get installed on a PC; Firefox, Google Chrome, OpenOffice, iTunes, Adobe Flash, Java, Adobe Acrobat, VLC, and WinZip. Then, I carelessly clicked on ad results, which appeared above or on the same first page as "real" search results. These paid ads were identified by notes and highlighted in a very pale color to differentiate them (slightly) from the actual search links that appeared nearby.

The ads didn't appear after every search and the ones that appeared varied among searches and were different for different browsers. Sometimes, the first paid ad link actually took me to the software's true source site (i.e. searching for Google offered www.google.com first). Often Avast would block a download it recognized as harmful, but Avast did not catch many problems.

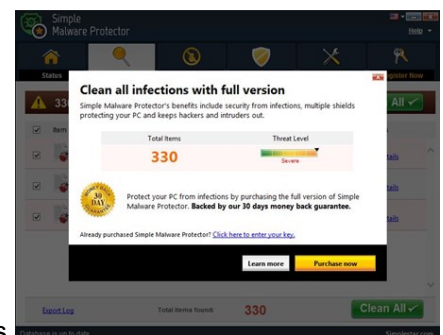
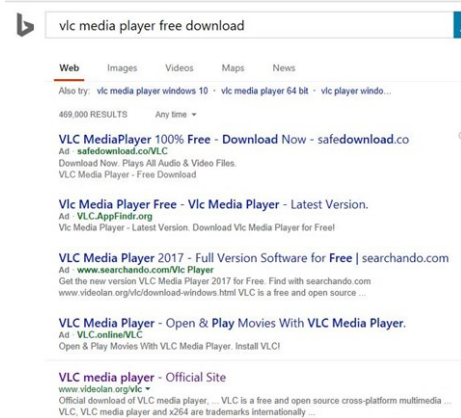
For all of the searched for programs, I was able to bring up more questionable sponsored search results within seconds of repeated searching. Misleading results showed up in all search engines and I could not determine that any browser offered better or worse protection than others.

For each ad link, I clicked through and installed the respective programs via the link or button provided. Instead of delivering just the application I was looking for, all of the paid links attempted to tack on unwanted programs. In some cases, if I was careful to read all of the fine print and uncheck boxes, I could get the files I was looking for without a bunch of extra "added value" software, but it was very difficult.

For the purposes of this article, I acted as an inexperienced user (or an experienced user who's not paying attention) and clicked my way through ads and dialogue boxes that looked like the End User License Agreement (EULA) we're used to seeing through when installing software.

### And ... They Got Me!

After installing just a few programs this way, I started accumulating browser toolbars (Bing, Yahoo, and Google) and noticed my search engine and home page had been hijacked to something unwanted. As I continued the process, Windows started slowing down to a crawl.

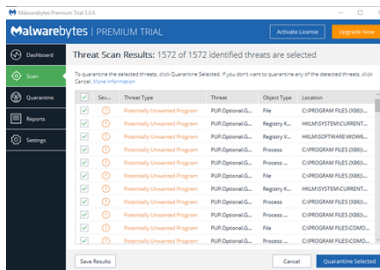


After installing all of the programs on my list, I opened Windows 10's Programs and Features (in the Control Panel) and each browser's extensions and add-ons and counted 39 items that had been installed in addition to the programs I intended to get. On rebooting, three new programs launched popup windows at startup, including two that started running virus/registry scans as soon as they launched, and a couple that flashed warning windows and offered fixes if I registered and/or upgraded to the full paid version.

Remember this was originally a clean install of Windows 10 that needed nothing.

Within a few minutes, my computer became noticeably slower, plagued by numerous popups, and was becoming essentially unusable.

A Malwarebytes scan disclosed 1572 unwanted programs were present on my system. I'm sure not all of these were nasty, but if even a small fraction of them were, I would be in real trouble.



### Conclusions and Recommendations

Most of us will occasionally have reason to download and install some third-party (non-Microsoft) software from the Internet. This does not have to be dangerous if you pay attention that the software is being offered from the true home site of that product. NEVER download software from any sponsored link unless the desired software creator is the sponsor.

Do not depend on your anti-malware program to protect you. It will catch some issues, but not all.

***This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.***

{Ed. note: The last statement is very true. No single security product will protect your PC 100%. Every software producer codes their individual product to act in a prescribed manner, and their product is copyrighted. So, each product performs differently, using unique methods to accomplish the same goal — to protect your computer. This is why it makes so much sense to use more than one anti-spyware product. I have used [Malwarebytes](#) (paid version) and [SuperAntiSpyware](#) ("free" version, not "trial" version) as my one-two punch for many, many years. It's not unusual to have one tool find something that the other did not. Ask several PC users, and you'll get a laundry list of other similar security tools. But it is always time well-spent to research your options. Keep in mind that you can only use ONE anti-virus product, but multiple anti-spyware products, on one PC.}



## File Extensions — Helpful or Not

by Jim Cerny, Forum Leader  
Sarasota Technology Users Group, Florida  
Sarasota Monitor [www.thestug.org](http://www.thestug.org)  
[jimcerny123@gmail.com](mailto:jimcerny123@gmail.com)

So someone sends you a file attached to their email — you try to open the file and you can't, why is that? I mean, they obviously could open the file on *their* computer, why couldn't you open it on *yours*? Unfortunately, this is the frustrating part about FILE EXTENSIONS (also known as "file types").

If you use a program to CREATE a file, it is nice to have the SAME PROGRAM to open or work with the file you created. Naturally, if you use your computer to create a file then your computer has the program needed to open the file later. The problem is when someone creates a file on their computer and sends it to you — you need to have a program that can open the file on your computer.

Let's look at one example: I have the Microsoft Word app (or program) on my computer and I create a new document with it. I save the document as a file, and the computer assigns it a "file extension" or "file type" of ".docx". The file extension is always the last three or four characters of the file name right after the dot. This indicates that this file was created using a recent version of Word. If I send this file (as an attachment to an email) to someone else and they do NOT have Word, they cannot open the file!

It is an option in Windows whether to display the file extension, so your computer may not show you the file extension as part of the file name. To see the file extension when you use File Explorer, open the File Explorer app, click on the "View" menu tab and check the box labeled "File Name Extensions". This will display the file extensions (file type) as part of the file name for all files.

Things have changed over the past few years as there are more options to open the file to READ it or to EDIT it. Your computer may suggest some internet sites or free apps that may be able to open the file for you.

A good app like Microsoft Word may allow you to save your file as a different type of file — so you can pick one that is easier for more people to open. You could save it as a ".pdf" or ".rtf" file type if you want. A ".pdf" file can be opened by many apps but usually, the contents, or text, of the file can NOT be edited, only read. The ".rtf" file type (Rich Text File) can also be opened by several other apps and can be edited, BUT the text will have lost any formatting or options used in Microsoft Word.

Are you working with photo files? Most photos or pictures today are saved as a ".jpg" file type and any app that can open or work with photos will be able to open this file. That's nice.

(Continued on page 9.....[File Extensions](#))

## How To – Keyboard Fix

By Dick Evans

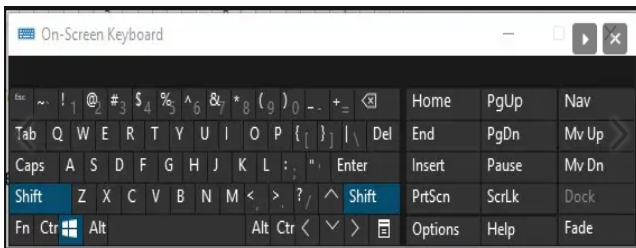
<https://davescomputertips.com>

Have you ever had a key on your laptop stop working? I mean, no matter how hard you hit it, nothing happened. If you have an extra keyboard you can always plug it into the laptop and use it instead of the one missing a key or two. There are other alternatives.

If your laptop has a numeric keypad and you know the ASCII chart, you can hold down the Alt key and enter the three-digit code for the character you need. For example, the letters A-Z are coded 065 to 090.

Try it. Hold down the Alt key and type a code on the numeric keypad in that range. Notice they are all capital letters. For the lower case letters, the range is 097 to 122. The entire chart can be seen at [asciitable.com](http://asciitable.com).

The numbers on top of your keyboard will not work with the Alt key.



In Windows 10 you have another alternative. Win+Ctrl+O will toggle a working keyboard to display on the screen. Then use the mouse to click the needed key. You can resize the keyboard and drag it to any position on the screen.

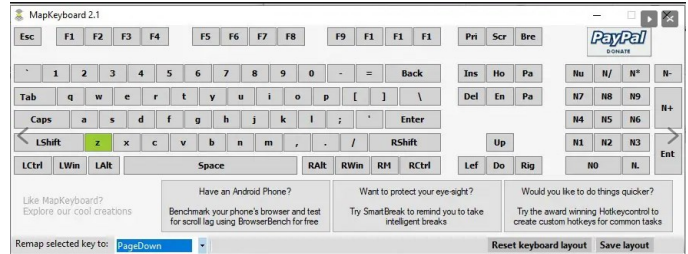
Another alternative is to reassign a seldom-used key to work instead of the broken one. For example, Page Up and Page Down and Pause keys and even Home and End might be reassigned. However, this cannot be accomplished in Windows itself unless you like to edit the registry file directly, which is not recommended.

I located a small program that allows you to do this called **MapKeyboard**. It is a quick download and does not need to be installed. Another one I found is called **SharpKeys**. The former was easier to use, for me.

Some like to remap the Caps Lock key to a Shift key or even turn it off so they don't hit it by accident.

In our example, we can use MapKeyboard to make one of our seldom-used keys to replace the broken one. Download the program and run it. It displays a keyboard and allows you to change the function of any key to any other key. You need to log off and back on to see the results.

In the example below, I clicked the letter 'z' and remapped it to use the PageDown key. Now my non-functioning z key is still not working but I can type the letter Z by pressing the PageDown key. Awkward, but workable.



I hope this has given you a tool to help others with keyboard issues.

***This article is republished, with permission, from the DavesComputerTips web site.***



*(File Extensions....continued from page 8)*

Here are just a few of the most popular file extensions (types):

- ◆ **.doc** or **.docx** – Microsoft Word
- ◆ **.html** – webpage
- ◆ **.jpg** – picture or photo image
- ◆ **.pdf** – a document file that can be opened or read by many apps but cannot be edited
- ◆ **.rtf** – rich text file that contains formatting (the Wordpad app creates these files)
- ◆ **.txt** – plain text file will no formatting
- ◆ **.xls** and **.xlsx** – Microsoft Excel spreadsheet

There are probably many thousands of different file types {see <https://www.file-extensions.org>}, but thankfully you do not have to know them all. If you have any questions about a particular file type, just Ask Google {*for any search engine*} and you will find out what apps could have created the file and which apps can open or work with that file.

I know this all sounds a bit confusing, but you should only run into a problem when you try to open a file that you did not create on your computer. Should this happen you may have to contact the person who sent you the file and ask them to send it to you again as a different file type – one that you know you can open.

Hopefully, you will become comfortable with the most common file types that you use. Remember you can always Ask Google {*or other search engine*} for help!

***This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.***

*{Ed. note: Two quick comments: PDF files can be edited. And files created with MS Office applications (Word, Excel, etc.) can be opened, read, and edited using other office suites (LibreOffice, OpenOffice, etc.)}*

## Windows Free Snip and Sketch Tool is New and Replacing the Old

By Jim Cerny, Forums Coordinator  
STUG Monitor [www.thestug.org](http://www.thestug.org)  
[jimcerny123@gmail.com](mailto:jimcerny123@gmail.com)

The new Windows “Snip and Sketch” tool was part of the Windows 10 October 2018 update. This tool is intended to REPLACE the old “Snipping Tool” of previous Windows editions. But they (Microsoft) did something to actually help us users this time – they kept the old tool! So you can play and learn the new Snip and Sketch and keep the old Snipping Tool too! Maybe they learned not to force users into using updated or changed apps right away – we need time to adjust and learn, right?



Everything you could do in the old Snipping Tool you can do in Snip and Sketch, plus you get a few more tools and options. Thankfully these new additions are easy to see and use, and they can be ignored if you do not want to use them. Microsoft promises more options to come. Be sure to search (the web) for videos on how to use Windows Snip and Sketch! I am including here only the basic options.



Click on the Windows logo in the lower-left corner of your desktop and you will find Snip and Sketch in the alphabetical list of apps that appear. It is not inside the Windows Accessories folder of apps (where the Snipping Tool still remains). I recommend dragging this app to your desktop screen to always keep it handy. But you can also open it anytime by holding down the Windows key + Shift key + S on your keyboard. Upon opening the app, your whole screen goes gray and you will see the small controls rectangle at the top. Here you select HOW you want to select what you want to snip or capture. From left to right you can select a rectangular area, freeform selection, the entire window, or your full screen. If you select the rectangle, you drag your mouse on the screen to select whatever you want. As soon as you release your mouse – presto, your selected image has been captured and saved on the clipboard to do with whatever you want!

You can open a Word document for example, place your cursor where you want, and “paste” your clip right in your document. Or you can open the Windows Paint app and you can “paste” it there if you want to do more editing. At the same time that your snip is placed on the clipboard, you will also see a message stating that you can edit, draw, or markup your selection. Click to do that and Snip and Sketch opens in its own window with its own menu of options.

Various easy marking tools are available for you to play with and try. There are highlighters and markers, and

clicking on the down arrows will open things like color choices, etc. Once you have “sketched” on your “snip” you can save it as a “.jpg”, “.png”, or “.gif” format by clicking on the old floppy disk save icon and selecting the file type you want.

The new Snip and Sketch is easy to use and very helpful for saving and sketching on any image on your screen for any purpose. Why not give it a try?

***This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.***

*{Ed. note: To keep the tool even more accessible, once you have the icon on the desktop, simply drag it down to the task bar (the long bar at the bottom of the computer screen), so that it's available there, too, with just one mouse click. I use it often.*

*This Snip and Sketch tool is particularly handy when you are in need of assistance with a feature or problem on your computer. For instance, if a pop-up window appears, and you don't know how to react to it, or how to use a particular visual program feature, just take a snip of it, save it as an image file (.jpg), and email it to someone for some direction or assistance.}*



*(Wi-Fi Security....continued from page 11)*

may be adequate for most home use. I can't prove it, but I have seen some research that showed that it would take a fast PC over 15,000 years to crack a WPA2 passphrase of only 10 characters. (Maybe you could do it in a year with 15,000 computers.) That kind of security would probably be enough for most of us.

So, now that we know what's behind Wi-Fi security, what shall I do about the original problem of what Security selection to use in place of WEP? Well, I guess the obvious answer is WPA2, as long as all devices support WPA2. Unfortunately, I may not find this out until I attempt to have all devices re-setup with WPA2. I only have a few devices that are older than six years old, so it may just work out. Wish me luck.

Postscript: The upgrade to WPA2 worked out just fine. Unfortunately, about 2 months later I had to replace the router. I had to do the whole upgrade all over again, so now I'm really good at updating all my Wi-Fi devices.

***This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.***



## Wi-Fi Security – Which One: WEP, WPA, or WPA2?

By Phil Sorrentino, Contributing Writer  
The Computer Club, FL

[www.sccccomputerclub.org](http://www.sccccomputerclub.org) [Philsorr@yahoo.com](mailto:Philsorr@yahoo.com)

Well, it finally happened. I tried to add another device to my home Wi-Fi network and I couldn't. I have been in fear of this happening for the last few years. No, it is not the fact that I tried to add one more device and that went over a limit. The limit on the number of devices you can have on a Wi-Fi network is only limited by the local IP addresses you set up, which was much higher than the number of devices I had on the network. I have had my current router since July 2010. I bought it shortly after the 802.11n standard found its way into reasonably priced routers (around 2009). The "n" version followed the "g" version and increased the bit rate (speed) from about 50Mbps to somewhere in the 100 to 300 Mbps area. (The actual speed you get from the router to a device is dependent on many things.) When I set up the router I had a few older (legacy) devices that I still used. Some of those older devices didn't support the latest Security. So when it came to set up Security for the network, I chose the older Security standard "WEP." Although WEP is not nearly as secure as WPA2, every device supported WEP so there was no problem, until today, when I tried to add a device that did not support WEP. The new device, a security camera, only supports WPA and WPA2. So, now I have to change the Security used by my router to either WPA or WPA2.

This may not sound like much of a problem, but once I change it in the router, I have to change every device that wants to use my Wi-Fi network. Yes, all the laptops and tablets, all the cell phones, all the Streaming devices, all the Smart TVs, all the smart bulbs and plugs, the wireless printer, any Wi-Fi extender access points, Alexa, Google Home, and all the phones and tablets owned by friends and family that use my Wi-Fi network when visiting.

The first thing I'll have to do is change the security used in the router. For this, I will need the Username and Password for the router. Many router's Username can be left blank and the default password is typically "Admin." (If you have changed either of these on your router, this is a good time to resurrect the correct Username and Password for future use.) Now, using a web browser, I'll go to the IP address of the router. Many routers use <http://192.168.1.0> or <http://192.168.1.1>. Once at the router page, I'll put in the username and password. Once in the router setup, I'll find Wireless or Wi-Fi Security and look for the Security type. Then I'll choose the desired Security type and put

in a passphrase. I'll make a note of the new Wi-Fi password for the future (a very important step). Now I can go around to all the devices that use the Wi-Fi and make the appropriate changes in their setups. Wish me luck.

So, what really is Wi-Fi security? Well, directly from Wikipedia "Wireless (Wi-Fi) security is the prevention of unauthorized access or damage to computers or data using wireless networks." Basically, Wi-Fi Security protects the data that goes between a router and a device. The device could be a computer, a wireless phone, a smart TV or DVD player, a smart LED bulb, any device that connects to the router, even a smart refrigerator.

The most common types of Wi-Fi security are Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA). WEP, which is the older standard (Circa 1999), provides fairly weak security. It is well known that the WEP password can often be cracked within a few minutes with a basic laptop computer and widely available software tools. WEP used a 64-bit (or 128-bit) encryption key. The key was manually inserted into the device and it remained constant. WPA was introduced around 2002 to solve some of the problems with WEP. Even if your router is six years old, it most likely supports WPA. WPA2 is a further improvement over WPA and is

the current Security standard. WPA2 employs an encryption algorithm that encrypts the data with a 256-bit key, the longest of all the keys used, and the longer the key the stronger the security. WPA also employs a per-packet key, meaning that it dynamically generates a new key for each packet that is transmitted. In early 2018, WPA3 was announced. WPA3 will have several security improvements over WPA2, but it will take some time for it to show up in routers and devices.

To use WPA or WPA2, you provide the router with a "passphrase" between 8 and 63 characters long – the longer the better. The passphrase can be a collection of alpha and numeric characters, including special symbols like \$, %, and #. (Actually, if you are familiar with the ASCII code, all ASCII printable characters, those decimal values between 32 and 126, can be used. Which, by the way, also includes "space".) The router will then use the passphrase and the network's name to generate unique encryption keys to be used on the network. The keys will constantly be changed to avoid being cracked. WPA2, the second version of WPA, uses a more advanced encryption algorithm that is more efficient and more resistant to cracking. (All Wi-Fi products have been required to support WPA2 since about 2016. It was intended that WPA2 essentially replace WPA.) Although it is true that "the longer the passphrase, the stronger the protection", it may not be the practical way to go. A passphrase only 9 or 10 characters in length

*(Continued on page 10.....Wi-Fi Security)*



## Are Identity Theft Protection Services Worth It?

By Bob Rankin

<https://askbobrankin.com/>

**Y**ou may be concerned about identity theft these days, and with good reason. If someone assumes your identity they can open new credit cards, raid your bank accounts, ruin your employment prospects, or even commit crimes for which you are blamed. With so much at stake, many people are paying \$20 or more a month for identity theft protection services. But are they wasting their money? Here's the scoop...

### Is Identity Theft Protection Effective?

Todd Davis, founder of identity theft protection service LifeLock, became famous for billboards that bore his Social Security Number and a dare to ID thieves: "Steal my identity" which was protected by LifeLock, of course. Well, it turns out they did, at least thirteen times! In 2010, LifeLock was ordered by the Federal Trade Commission to pay more than \$12 million in fines for false and misleading advertising.

Although LifeLock has since changed their advertising and the means they use to spot identity fraud, no identity theft protection service can absolutely ensure that your identity will not be stolen! In fact, LifeLock's own advertising carries the disclaimer that "no one can prevent all identity theft or cybercrime, and LifeLock does not monitor all transactions at all businesses."

The problem is that your identity can be vulnerable to theft from sources far outside of your control, or even sources that you don't know about. Most data breaches occur at merchants, service providers, government agencies, and other institutions to which you have given your personal information, and at still others to whom those entities have given your information without your knowledge.

Most people's identities are exposed to theft in so many different places that it is impossible to protect them all. You have to rely upon the security measures taken by those entities to protect you. Until quite recently, many business, government offices, and even one credit bureau were lax about protecting personal information from theft. (See [Equifax Takes The Data Breach Cake](#).)

According to researchers, about 10% of Americans fall victim to identity theft each year. The [Identity Theft Research Center](#) reports that there were 1244 security breaches involving the theft of over 440 million sensitive records in 2018, the last year for which reporting was released. Major retailers, banks, government agencies, utility companies, schools, and other institutions left the doors open in often stupendously stupid ways. There is nothing that LifeLock or any other identity theft protection service can do to force third parties to protect your data. So what do you get for your subscription fee (or "insurance policy")?

### What Protection is Actually Offered from Identity Theft?

LifeLock and its competitors monitor the activity of your identity online and in the economy. They monitor applica-

tions for credit cards, bank accounts, and other financial instruments made in your name. They look for "unusual activity" and alert you to it; effectively asking, "Hey, did you really do this?" If you didn't, then some thief may have, and it's time to hit the panic button.

If it appears that your identity has been stolen and is being misused, LifeLock can take care of alerting credit card companies and other institutions for you. Accounts can be locked or closed; new credit cards issued; and other measures taken to thwart thieves' use of your identity. But that won't stop a shoplifter who's caught by police from giving them your name and address as his own.

Repairing the damage done by identity theft is a years-long, painful, and expensive process. Some things that you never did may remain on your record forever. In one case, a sex offender used another man's identity, and the innocent man was told by authorities that his name can never be removed from databases of sex offenders.

LifeLock and others in the fraud protection business promise to help you repair the damage if you are a victim of identity theft. But how far they'll actually go depends on where you live, and the plan you've selected. The LifeLock Terms of Service is 8,297 words of legalese, and the document entitled [Evidence of Coverage: All Members Except NY and WA State Residents](#) spells out how much they will pay out to help you, based on your membership in one of the 27 plans listed. And in the Exclusions section, you'll find that the policy does not cover losses not reported within ninety days, or "loss or damage resulting from or arising out of a Cyber Attack."

I don't personally know anyone who has suffered from identity theft while a LifeLock subscriber, and then tried to submit a claim for help. I do know one person who suspected that her mother (a LifeLock subscriber) had become an ID theft victim. Fortunately, it was a false alarm. But she says that LifeLock certainly did everything she would have wanted, when it came to investigating the situation, and that gave her confidence that LifeLock would have honored their guarantee if there had been a real problem.

Here's the bottom line... Identity theft protection services can provide you with some protection from identity theft, but they cannot guarantee that it will never happen. And if it does, they will provide some assistance in cleaning up the mess, but don't expect them to make it like it never happened. You'll have to decide if that's worth the \$15 to \$35 a month that may cost.

***This article is republished, with permission, from the Ask Bob Rankin web site.***

*{Ed. note: These services can't always prevent your identity from being compromised, but can take much of the pain and time out of getting your identity re-established. But when such services claim that they spend 'up to \$1 Million' to do so, that simply means that they will spend somewhere between 1 dollar and 1 million dollars on your case.}*



## Use This Hidden Keyboard Combo to Fix Your Frozen Computer

by Ben Stegner

<https://www.makeuseof.com>

Having your PC suddenly freeze in the middle of working is frustrating. Windows can become unresponsive for many reasons, but there's a little-known shortcut that can help you recover from one common cause.

We'll introduce a new handy keyboard shortcut you probably don't know about, then discuss a few more quick tips for getting your frozen computer running again.

### The Hidden Keyboard Combo for Fixing Freezes

Windows offers a standard shortcut that will restart your video drivers. You can use it anytime by pressing the key combination Win + Ctrl + Shift + B.

Once you do so, you'll see your screen go black for a moment and hear a beep while the video driver resets. After a second or two, your display will return. Since this only affects your graphics drivers, all your open apps remain exactly where you left them. You won't lose any work.

Many of you have seen the stories about video issues in the April Win 10 update & that you can press Shift+Ctrl+Win+B to fix it. Well, occasionally I have issues with my docked laptop and external monitors coming back on after sleep. This fixes it! Handy outcome from this mess.

This only works on Windows 8 or 10, so Windows 7 users can't take advantage of it. However, it will work no matter what kind of graphics drivers you have. Nvidia, AMD, and even Intel integrated graphics will all reset just fine.

### Other Troubleshooting Tips for Frozen Apps

Depending on the cause of the freeze, this shortcut may or may not fix your issue. If your graphics driver gets stuck, restarting it should let you continue on without having to restart your computer.

But if this doesn't work, you should try pressing Alt + Tab to switch to another program. Still stuck? Try Ctrl + Shift + Esc to open the Task Manager so you can kill any unresponsive programs.

Should neither of these work, give Ctrl + Alt + Del a press. If Windows doesn't respond to this after some time, you'll need to hard shutdown your computer by holding the Power button for several seconds. This is akin to pulling the plug, and is the only way to escape a system freeze.

***This article is republished, with permission, from the MakeUseOf web site.***



## Web Page Reviews Overload

(Web sites that did not fit on page 14)

Whether sanctioned by the government or just by dedicated social groups, every day is a 'national day' for something. (Even a National Grilled Cheese Day.) Here is a list, in case you feel like celebrating something.

<https://www.whatnationaldayisit.com>

Each day, a different encore presentation from the Metropolitan Opera company's *Live in HD* series is being made available for free streaming on the Met website, with each performance available for a period of 23 hours, from 7:30 p.m. EDT until 6:30 p.m. the following day. Includes outstanding complete performances from the past 14 years of cinema transmissions, starring all of opera's greatest singers.

<https://www.metopera.org/user-information/nightly-met-opera-streams/>

This VPN glossary gives you useful terms and what they mean for your privacy. (Do you know that your ISP can track all of your web surfing and sell that knowledge?)

<https://www.cnet.com/news/all-the-vpn-terms-you-need-to-know/>

Best *free* VPNs: 5 reasons why they don't exist.

<https://www.cnet.com/how-to/best-free-vpns-5-reasons-why-they-dont-exist/>

Free education and entertainment content from the DIA.

<https://www.dia.org/athome>

Tax changes and key amounts for the 2020 tax year.

<https://www.kiplinger.com/slideshow/taxes/T055-S011-tax-changes-and-key-tax-amounts-for-2020/index.html>

Your data is shared and sold...What can you do about it?"

<https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/>

Back around the 1980s, before PCs and tablets and cell phones, this is what we bought to play electronic games.

<https://handheldmuseum.com/>

Google says it doesn't 'sell' your data. Here's how the company shares, monetizes, and exploits it and compromises your privacy.

<https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and>

How to use dictation to talk instead of typing text in Windows 10. (Be sure that the microphone is 'on' in Windows' Privacy Settings; remember to turn it 'off' later.)

<https://www.tenforums.com/tutorials/108910-how-use-dictation-windows-10-a.html>

Library containing thousands of file extensions with detailed descriptions, including their current use and list of programs that can open, view, edit, convert or play them.

<https://www.file-extensions.org/>

## Web Page Reviews

by Paul Baecker — [webwatch@sterlingheightscomputerclub.org](mailto:webwatch@sterlingheightscomputerclub.org)



This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything.

**Club members only** are encouraged to submit favorite sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG issue. Also check the SHCC web site (“Web Page Reviews”) for previous gems.

7 free Skype alternatives for a Windows or Linux PC.  
<https://www.makeuseof.com/tag/skype-alternatives-windows/>

12 world-class museums you can visit online. When visiting museum sites, look for links like ‘collections’ or ‘galleries’ to view what is offered for free viewing.  
<https://www.mentalfloss.com/article/75809/12-world-class-museums-you-can-visit-online>

Construction of the Panama Canal from 1904 to 1915; sections with historical background, images, and some interactive activities (like map and timeline).  
<https://panama.lindahall.org/>

Enormous collection of live-cams in natural locations — bears, birds, oceans, eagles, dogs, cats, much more.  
<https://explore.org/livecams>

This *Tiger Funnies* YouTube channel offers all sorts of comically entertaining videos.  
<https://www.youtube.com/channel/UCR2KG2dK1tAkwZZjm7rAiSg/playlists>

How to sanitize and clean your phone. We all know how yucky they can get.  
<https://www.maketecheasier.com/sanitize-clean-your-phone/>

Free games you can play when you’re stuck inside.  
<https://www.gamespot.com/articles/free-games-you-can-play-right-now-gears-5-uncharte/1100-6474874/>

Just got a new TV or streamer device? You need to change these privacy settings.  
<https://www.cnet.com/how-to/just-got-a-new-tv-or-streamer-you-need-to-change-these-privacy-settings/>

How to reset a forgotten root password in Linux Mint.  
<https://www.tecmint.com/reset-forgotten-root-password-in-linux-mint/>

The National Gallery of Art offers virtual tours of their works. Start with the “Collection’ or ‘Exhibitions’ options.  
<https://www.nga.gov>

Simple calculator for how much toilet paper you need.  
<https://howmuchtoiletpaper.com>

Do the bright screens of Windows’ File Explorer, your browser, and Office applications blind you? Try enabling “dark themes”.  
<https://www.howtogeek.com/222614/how-to-enable-windows-10s-hidden-dark-theme/>

7 Skype tips and features you might have overlooked.  
<https://www.makeuseof.com/tag/skype-tips-features/>

How to sanitize and clean your laptop. Get the nasties out  
<https://www.maketecheasier.com/sanitize-clean-laptop>

Watch the otters live at the Detroit Zoo enjoying themselves, despite the absence of visitors to show off to.  
<https://detroitzoo.org/otter-live-cam/>

Learn how to view and reduce the amount of “diagnostic data” that Microsoft takes from your Windows 10 PC.  
<https://www.groovypost.com/howto/use-diagnostic-data-viewer-windows-10-1803/>

7 free Skype alternatives for a Windows or Linux PC.  
<https://www.makeuseof.com/tag/skype-alternatives-windows/>

Simple calculator for how much toilet paper you need.  
<https://howmuchtoiletpaper.com>

Do the bright screens of Windows’ File Explorer, your browser, and Office applications blind you? Try enabling “dark themes”.  
<https://www.howtogeek.com/222614/how-to-enable-windows-10s-hidden-dark-theme/>

7 Skype tips and features you might have overlooked.  
<https://www.makeuseof.com/tag/skype-tips-features/>

How to sanitize and clean your laptop. Get the nasties out  
<https://www.maketecheasier.com/sanitize-clean-laptop>

Watch the otters live at the Detroit Zoo enjoying themselves, despite the absence of visitors to show off to.  
<https://detroitzoo.org/otter-live-cam/>

Learn how to view and reduce the amount of “diagnostic data” that Microsoft takes from your Windows 10 PC.  
<https://www.groovypost.com/howto/use-diagnostic-data-viewer-windows-10-1803/>

7 free Skype alternatives for a Windows or Linux PC.  
<https://www.makeuseof.com/tag/skype-alternatives-windows/>

How to sanitize and clean your phone. We all know how yucky they can get.  
<https://www.maketecheasier.com/sanitize-clean-your-phone/>

Free games you can play when you’re stuck inside.  
<https://www.gamespot.com/articles/free-games-you-can-play-right-now-gears-5-uncharte/1100-6474874/>

Just got a new TV or streamer device? You need to change these privacy settings.  
<https://www.cnet.com/how-to/just-got-a-new-tv-or-streamer-you-need-to-change-these-privacy-settings/>

How to reset a forgotten root password in Linux Mint.  
<https://www.tecmint.com/reset-forgotten-root-password-in-linux-mint/>

The National Gallery of Art offers virtual tours of their works. Start with the “Collection’ or ‘Exhibitions’ options.  
<https://www.nga.gov>

Simple calculator for how much toilet paper you need.  
<https://howmuchtoiletpaper.com>

Do the bright screens of Windows’ File Explorer, your browser, and Office applications blind you? Try enabling “dark themes”.  
<https://www.howtogeek.com/222614/how-to-enable-windows-10s-hidden-dark-theme/>

7 Skype tips and features you might have overlooked.  
<https://www.makeuseof.com/tag/skype-tips-features/>

How to sanitize and clean your laptop. Get the nasties out  
<https://www.maketecheasier.com/sanitize-clean-laptop>

## Web Watch Column on the Club Web Site

Check out the **WebPageReviews** section on the club’s web site. There you can see past web sites reviewed in this column. They are arranged into various *keyword* categories to help locate a specific topic or site.

**NOTE: Many of the links in the digital newsletter connect to the Internet if clicked. For those that do not, copy and paste the link into your Internet browser.**