The Space Coast PC Journal

Windows Defender Bug Fills Hard Drive

by John Lister

Komando.com

A bug with Windows Defender has been filling computers with thousands of largely useless files. The bug is fixed with the latest update and this is definitely an application worth keeping updated.

Windows Defender (officially known as Microsoft Defender Antivirus) is the built-in security tool in Windows 10. The consensus view is that it's not as good as the best third-party tools, but does a decent job and is certainly a useful line of defense for the average user.

Unfortunately a recent update, which took Windows Defender to version 1.1.18100.5, introduced an annoying bug. Users noticed a problem with a file folder located on most machines at C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store, which may need administrator privileges to access.

30GB Of Unwanted Files

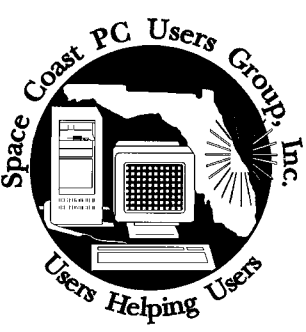
This folder should contain a few files which relate to previous scans. There's not a great deal users can do with them as they aren't in a format accessible by other applications. Generally the files are a couple of kilobytes at most and thus users can safely ignore them.

The problem is that on some machines literally thousands of the files have been generated. In the most extreme case reported they totaled 30GB. As Bleeping Computer notes, that could be a significant problem for people who use a small drive for Windows and programs and a larger one for documents and data. (Source: bleepingcomputer.com)

Continued.....page 4

The Monthly Publication of the Space Coast PC Users Group, Inc.

Visit Our web Site at www.scpcug.com



July 2021 Vol.XXXVII Issue VI I

Submitting Articles to the Journal

We encourage all of our members to submit original computer-related articles for publication in *The Space Coast PC Journal*.

Writing a Product Review

It is really not that difficult to write a good review for *The Space Coast PC Journal*. These guidelines will help you get started:

Product information

- List the product name, release level, and manufacturer.

Use

- What does this product do?
- How easy is it to learn and use? Is it for beginners or does it have advanced features?
- List and describe some of the features. If this is an upgrade, what is new to this version?
- What did you like or dislike about it?
- Did you have to call Customer Support? What for? Were they helpful?

Installation

- How much disk space did the product take?
- How long did it take to install?
- Was it difficult to install?
- Specify requirements such as: DOS level, Windows level, Windows type, etc.

Recommendations

- Would you recommend this product?

Remember these are guidelines. They are not meant to be all-inclusive, nor should they limit your creativity. But all of them should be included as part of your article. Then the review will practically write itself!

Preparing Your Articles

To assist us in incorporating articles into the *Journal*, it would be helpful if certain minimum standards were followed. Use this quick-step guide:

Format: The preferred format is ASCII text files.We can also work with other formats, but check with the editor before using them.

Text: Single-space the text—even between paragraphs. Don't indent paragraphs. Use hard returns only at the ends of paragraphs.

Use only one space after periods, colons, and question marks. Follow standard capitalization rules.

Use left justification only. Do not right justify or block your text. (Word processors add extra spaces between words to justify the text and each of those extra spaces must then be removed.

Graphics: The preferred format for graphics accompanying your text is TIFF—in separate files from the text. Embedded graphics are not useable. Most image editing programs have a "resize" option to alter the size of graphics. Please try to keep your graphic file sizes to around 1 meg in size. Call the editor if you have questions.

Be sure to include your name and phone number so we may contact you if we have any questions. Anonymous articles will not be published.

Submit your article by uploading the file to ringram728@earthlink.net or bring your disk and hardcopy to the Monday meeting or mail to:

Editor, SCPCUG Journal
Space Coast PC Users Group, Inc.
1360 Mayflower Avenue
Melbourne, Fl 32940-672

3Articles must be received by the 28th of the month to appear in the next issue, and all are, of course, subject to editing. □

From The Editor

You're looking at what is one of the final issues with me as editor. After some 20 years in this capacity I've reached the point where it's time for someone else to take on the chore.

Barbara Mead has stepped up to take on the job. We discussed it for a spell at the last Learning Center session. ..

It's quite possible that there will be significant changes in the appearance of the Journal. Barabara is not familiar with the Adobe Indesign program which I have been using since Adobe Pagemaker 7 was replaced.

The question remains as to which softwarre she will be most comfortable using. I can provide her copies of all that I have been using. But she is more familiar with the Microsoft Publisher.

Should that be the final choice, the appearance of the Journal may change drastically. So too may the content differ. That will all be up to Barbara when she takes over. I'll do all I can to make the transition as trouble-free as possible.

Ron Ingraham, Editor

The Space Coast PC Journal
Published monthly by the
Space Coast PC Users Group, Inc.
1360 Mayflower Avenue
Melbourne, Fl 32940-6723

Those who have listed an e-mail address would prefer to be contacted by e-mail rather than by phone whenever possible.

CLUB OFFICERS

President	Dan Douglas	datadan@msn.com	301-1075
Vice President	Larry Bennett	lbennett@qualitek.biz	259-2400
Secretary	Barbara Mead	rtr250@msn.com	427-4484
Treasurer	Irene Nelson	irenelnelson@gmail.com	806-4032
Journal Editor	Ron Ingraham	ringram28@cfl.rr.com	777-2578
Web Master	Curt Potsic	cmpotsic@att.net	632-7185
Membership Chairperson	Linda Glassburn	glassburn@earthlink.net	216-334-7555

STAFF MEMBERS

Hospitality	Barbara Mead
New Member Orientation	OPEN
Orientation Hostess	OPEN
Publicity	Larry Bennett
Help Desk	OPEN
Facilities	OPEN

HELPLINES

Internet/HTML	Curt Potsic	cmpotsic@att.net	632-7185
Windows10	Curt Potsic	cmpotsic@att.net	632-7185
General Computer Us	Tom Marr Calling Hours 10-6	yjm1938@yahoo.com.	338-5414

If there is a progam not listed that you feel comfortable with, let us list you as one of our helplines contact ringram28@cfl.rr.com

The SCPCUG Home Page is at:
http://www.scpcug.com
Check it out!!!!!

IN THIS ISSUE

Feature Articles

Regular Articles

Notices

Presentation
In Conference Room
2 PM
Get Together Welcome

Bring Some Friends

Windows Defender Bug.....from page 1

Update Should Fix Problem

The good news is that the problem appears to be fixed with a new update taking Windows Defender to version 1.1.18100.6. Windows Defender should keep itself automatically updated, but users can check which version they have by clicking on the cog icon for Settings within the Windows Security tool. (Source: express.co.uk)
If necessary, users can manually trigger an update through the Windows Update tool by looking for an update listed as "Security Intelligence Update for Microsoft Defender Antivirus."

It's not yet clear whether the fix in the update will clear out the unwanted files. If not, it appears safe to carry out a full scan in Windows Defender then empty the C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store folder. However, users may want to take a backup of the files to an external drive and keep it safe for a few days until they are certain Windows Defender is still running normally.

What's Your Opinion?

Have you spotted this problem? Do you pay much attention to Windows Defender? Should Microsoft warn users of such bugs or is it simpler just to concentrate on fixing them through updates? ❑

Relief On Hand From Endless Video Meetings

by John Lister

Microsoft is to make it easier to build breaks into videoconferencing schedules. The move is designed to overcome a mismatch between technology "efficiency" and the real world.

Automated scheduling tools make sense as a way for businesses to efficiently find and arrange times for people to get together. By default, most tools will schedule a meeting for a "round" time period such as 30 or 60 minutes.

From the Cashier's Cage

Financial Report for Month Ending June, 2021

CHECKING	
Beginning Balance	608.62
Snack Fund Donations	8/00
Ending balancee - includes $26.41 snack fund balance.	616.62
SAVINGS	
Beginning Balance	305..29
Interest	.01
Ending Balance	305.30
Total Accounts Balance	**921.92**

In an era when the vast majority of meetings were in person, that wasn't necessarily a problem. Back-to-back meetings were rare and even when they happened, meetings would naturally end a few minutes "early" to account for the fact people might have to physically relocate to their desk or a different meeting room.

That's not worked so well for businesses that now do most or all of their work online. Because people are now more comfortable with online meetings, it's more common to have two or three scheduled in a row. Meanwhile meeting leaders may be less likely to wrap things up early when they know that "getting" to the next meeting simply involves clicking a link and not even leaving a chair.

Auto-Breaks Offer Relief

That's led to some employees complaining of burnout when they are sat in back-to-back meetings without either a physical or mental break.

Microsoft is now tweaking Outlook so that both individual users and, perhaps more importantly, businesses as a whole can change the default scheduling settings. They'll be able to automatically build in breaks at the beginning and end of any scheduled meeting.

Users can choose between having a default break duration or having it vary depending on how long the associated meeting runs. (Source: theverge.com)

Wellbeing Boosted

Meanwhile Microsoft's Teams video meeting software is getting some "wellbeing" features added including optional meditation and mindfulness routines that are available to run before a meeting.

There's also a "virtual commute" feature that encourages the users to mentally review their work from the day, prepare their tasks for the following day, then go through relaxation exercises. The idea is to simulate the natural transition between work and personal life than some workers report is harder to achieve now they don't have a physical commute. (Source: onmsft.com)

What's Your Opinion?

Are these features worthwhile? Have you experienced online meeting fatigue? ❑

Dan's Desk

The big news announced this week was the upcoming release of Windows 11. Windows 10 was introduced back in 2015 and was said to be the last version of Windows. It appears that 'last' really meant 6 years!

From the introduction slides that Microsoft showed on June 25, Windows 11 definitely has a new look, that some have described as adopting many features and appearance that are familiar to Apple Mac OS users.

The schedule for release starts with a beta version, available to those on the Windows insider program starting early July, with the full release arriving before the end of December.

Microsoft said it would be a free update to everyone on Windows 10 when released. Anyone still running Windows 7 or 8 would be well advised to upgrade to Windows 10 prior to December to ensure they can upgrade to Windows 10 with no new license fees required.

Contact me if you need to know how to proceed from the older versions of Windows to get on Windows 10 which will be supported through the middle of 2025.

There was a discussion recently at one of our meetings concerning ways to capture videos being displayed on your PC. I have personally used a few 3rd party programs to accomplish this. The ones that come to mind are Screencast-O-Matic and Video Downloader Ultimate.

There is a free video capture tool built into Windows 10 as well. By pressing the Windows key and the G key, the capture tool will come up. Select the option to capture the screen as a ***game*** and the video can be saved.

I prefer the Video Downloader Ultimate tool which is linked to your browser (Chrome, Edge, etc.) and will start automatically. When you display a page that has video content, the tool displays the various formats and resolutions for the video(s) so you can choose which one you want to save.

It works with all common file formats and you can easily eliminate small files which are ads or non-primary files for saving.

If you have suggestions for other topics like this, that you would like to see explained, please let me know! ❑

Webmaster Wanderings

Due to Merritt Island Public Library Auditorium renovations there were no meetings at the library on Apr 15, Apr 17 and May 1. The Apr 15 Main Monthly Meeting was held virtually via the Zoom App with great success. Based on that we attempted to have the Apr 17 Learning Center Meeting via zoom but only 3 members participated. We therefore cancelled having a May 1 Learning Center meeting via Zoom. Our May 15 Learning Center Meeting was held in the Library Conference Room as the Auditorium renovations were not yet completed. There is now no current prediction as to when the Library auditorium renovations will be completed. Definitely not in May. So for now all meetings will be in the Conference Room.

Cutting the Cord - Watching TV (Legally) Without Cable - Held Apr 14, 2021

Video at: https://www.youtube.com/watch?v=eeWU4JcR0lY

Journal Current Issue page: The Space Coast PC Journal for June is now posted on scpcug.com where 12 past issues are also posted. All posted issues are available for download or reading online.

The Following Are All Special Events Page Updates

Jere's Tech Tips

Windows, Android, Linux tips from Jere Minich, APCUG Advisor, Region 5 (AL, FL, GA, SC).

New items include:

8 Google Searches that Put Your Privacy and Security at Risk

Stop Suffering from a Slow PC. 8 Surefire Ways to Speed It Up Yourself

Two-Factor Authentification: Who Has It and How to Set It Up

Google is Going to Make You Use 2FA Whether You Like It or Not

What is USB-C? An Explainer

How to Block Unknown Callers with Your SmartPhone

The 8 Best Android Apps to Save Content for Offline Viewing

5 Ways to Keep Your Online Searches Private.
https://apcug2.org/jerestips/

Learning Linux #6 -Settings & Files & Commands, Oh My -Held Mar 17, 2021 Video at: https://www.youtube.com/watch?v=L5v4iJbP-FI

Easily Stay In Touch With Your Members With Mailchimp -Held Mar 24, 2021 Video at: https://www.youtube.com/watch?v=YExxSE3-Ivg

How & Why To Back Up Your Hard Drive -Held Mar 31, 2021
Video at: https://www.youtube.

Continued.....page 8

Webmaster Wanderings.....

Cutting the Cord - Watching TV (Legally) Without Cable - Held Apr 14, 2021 Video at: https://www.youtube.com/watch?v=eeWU4JcR0lY

1 New Link

Review Geek - Make Gadgets Fun Again. Has categories of Latest News, Roundups, Reviews, Explore (SmartHome, Phones, Chargers, Gaming, Deals, Buying Guides, etc.), and Free Newsletter. https://www.reviewgeek.com/

Review Geek is a technology & gadget website with a singular focus: saving you time & money. We spend hours researching, testing, breaking, fixing, & re-testing a mountain of products, so you don't have to. Whether you're standing in a store aisle debating between products on the shelf or shopping in bed with your phone, we're here with the best recommendations, tips, & reviews. Review Geek has millions of readers, & our articles are distributed to hundreds of thousands of email subscribers every day.

Misc Items

The Killing of Adobe Flash on Windows 10

Adobe removed Flash from its Reader & Acrobat PDF programs in November 2020 and stopped support in January 2021. Now in July Adobe will start removing its Flash Player plugin from Windows 10. A few-months ago Microsoft released an optional update to remove the 32-bit Adobe Flash plugin & prevent a reinstall. Starting in June Microsoft will be issuing an update for total removal of the Adobe Flash Player. This will be included in a Preview Update for Win10 ver 1809 and above plus every subsequent Latest Cumulative Update. In July the FlashPlayer Removal Update will be included in the Latest Cumulative Update for Win 10 ver 1607 and ver 1507. Also, when you will be allowed to update to Win 10 ver 21H1, Flash will automatically be removed. Windows 10 currently runs on over one billion devices. Hopefully they will soon all be free of Adobe's Flash security risk.

Verizon Sells AOL and Yahoo

How times change! Remember AOL? It was how people connected to the Internet a few years ago & Yahoo was its front page. At their peaks, AOL had a market capitalization of more than$200 billion (Dec 1999) & Yahoo more than $125 billion (Jan 2000). Verizon bought AOL in 2015 for $4.4 billion & spent another $4.5 billion in 2017 for Yahoo. Verizon has now sold its AOL & Yahoo properties to Apollo Global Management. The deal is said to be worth $5 billion. That is about half of the nearly $9 billion Verizon originally paid for the two. Verizon will still maintain a 10% stake in the resulting company, now known as Yahoo. This deal is still subject to closing conditions. When completed it'll bring to an end Verizon's troubled experiment with media production & advertising.

Amazon Echo Show Is Now A Security Camera

Amazon never ceases to amaze me. Back in January I ordered a 1st generation refurbished Echo Show from woot.com on sale for $34.99. Figured that was a great deal as the original price was $229.99 when it was first released on June 28, 2017. The Echo Show is basically an Alexa Smart speaker with Video via a 7-inch touchscreen. You can read more about it on Wikipedia at https://en.wikipedia.org/wiki/Amazon_Echo_Show. The addition of video gives so much more capability to Alexa. Instead of just getting a voice response to

a question you also get a visual response. Amazon has also been adding capabilities to the Alexa App which I have on my Windows 10 PCs, Android Tablet, and Android Tracfone. Recently on a trip to the Tampa area to visit our son David and his family I decided to see if I could remotely view my kitchen using the Communication Drop-in option. Although Drop-in is basically designed to work as 2-way video call, it worked amazingly well on my laptop, tablet, and cellphone for seeing my kitchen remotely. I muted my video and audio so they would not be transmitted to the Echo Show. Now Amazon has has enhanced this type of remote monitoring by including a Home Monitoring Option on the Echo Show. This article from c/net "**Alexa has a new, hiddensuperpower: Transforming into a security camera"** at https://www.cnet.com/home/smarthome/ alexa-has-a-new-hidden-superpower-transforming-into-a-security-camera/ gives you all the details. There is one correction to the **setup** that I found. (Don't know if this might vary by generation.) The article says to go to **Settings** and there you should see a **Home Monitoring** switch to toggle on. At first I did not see the Home Monitoring switch. Then I discovered it when I first clicked **Camera.** So the sequence for me was **Settings, Camera, Home Monitoring.** ❑

RANSOMWARE 'THREATENS SAFETY AND HEALTH OF AMERICANS'

The growth of ransomware has reached crisis proportions to the point where it "jeopardizes the safety and health of Americans."

That was then-US Acting Deputy Attorney General John Carlin speaking a couple of weeks ago as he announced the launch of a new Department of Justice (DOJ) task force to tackle what is becoming one of the biggest malware crimes in the nation.

In fact, since we last wrote about the scam five years ago, the annual cost of ransoms to US citizens and organizations has ballooned from a few million dollars to several billions. One forecast suggests the total cost this year could be around $20 billion.

Businesses and public organizations like health and local government authorities are the main targets, shelling out as much as $20 million or more to get back access to their operating systems and frozen data.

Carlin says the affected organizations often pay up because they know the costs of damage from being locked out from their data could be many times higher than the amount of the ransom.

Organized crime gangs in China, Russia, and Eastern Europe are the main perpetrators. But individuals are also seeing a big uptick in ransom attacks, mostly from the Indian subcontinent and small gangs in the US.

Individuals usually face a ransom demand of between $500 and $1,000 payable in Bitcoin cybercurrency. Even if they pay, there's no guarantee the scammers will remove their lock. After all, they're crooks!

Consumers are also in danger when, as has happened, health service networks are attacked. This runs the risk that patients' health records and crucial monitoring and procedural programs are not available because files are locked up.

As you likely know by now, ransomware involves a hack attack or malware upload that, when activated, encrypts (jumbles and makes unreadable) the contents of a disk or even an entire network until a ransom is paid, usually in an untraceable format such as cybercurrency.Most recently, home users have been targeted with a fake Microsoft Windows update that arrives by email and as a pop-up on infected websites.

"By any measure, 2020 was the worst year ever when it comes to ransomware and related extortion events," Carlin said in the Wall Street Journal. "And if we don't break the back of this cycle,

Continued.....page 10

a problem that's already bad is going to get worse."

One reason things might get worse is that people and organizations continue to pay their ransoms. As long as that happens, the crime is bound to grow. Some observers believe the only solution is for it to become illegal for organizations to pay up.

Ransomware payloads can be planted on corporate networks by hackers. But with home users, they usually arrive on personal computers via email links and attachments. Despite countless warnings, users still click on them, often because they are cleverly disguised to look like genuine communications.

100 MILLION ATTACKS

Big organizations use security specialists, purpose-designed toolkits, and other safety routines to protect themselves. But they still get caught out. So, what chance is there for the rest of us to stay safe?

Many consumer Internet security providers are now including ransomware protection inside their software suites, underlining the importance of not only having one of these programs installed but also of ensuring it's regularly updated.

Computer security firm Trend Micro says it has blocked more than 100 million ransomware attacks in the past five years. During that time, the attack level has increased fifteen-fold.

These suites also include the ability to schedule regular backups so that if a ransomware attack succeeds, a user can reinstate an earlier backup.

However, "sleeper" ransomware could pose a new threat. After being installed on a system, it could remain dormant until activated sometime later. If malicious code is present but "sleeping" on a computer, it might also be copied onto a backup and activate when this is reinstalled.

Not surprisingly, therefore, a number of new services are appearing that claim to be able either to unfreeze a ransomed machine or at least recover locked-out data. But no one has yet come up with an infallible protection and recovery routine.

Some of the big names in software, like McAfee and Microsoft, also set up their own task force at the end of last year to tackle the issue. Security industry watchers are hoping this group will join up with the new DOJ team and work together rather than duplicating each other's efforts.

5 IMPORTANT ACTIONS

In the meanwhile, here are the 5 most important actions you can take to protect yourself from a ransomware attack and its effects.

1. Install and update security software as mentioned above. Here's a useful guide to some of the latest and best anti-ransomware products: The Best Ransomware Protection for 2021.

2. Take and keep regular system backups so that, even if your last backup was infected, an earlier one may be "clean." These should be stored on a separate device, disconnected from your PC or network, such as a removable drive, and preferably stored elsewhere.

3. Store your data -- documents, photos etc. -- on a separate disk or partition from your main operating system. That way, even if you lose access to your operating system, your data files might remain intact.

0. Avoid automatically clicking on links and attachments with emails, even if they appear genuine. If you can, take the time to check with the supposed sender.

0. In a worst-case scenario, where you lose valuable programs and data, or when the crooks fail to unlock, it may be possible to dis-encrypt the ransomed material. There are some specialist products for this but, generally, you will need to call in a professional. Even then, there's no guarantee it will work.

Should you pay a ransom? It's a tough call. However, the FBI is clear in recommending victims not pay. Plus, security experts at CyberEdge Group say that less than one in five victims who do pay get their files back.

Furthermore, as extortion victims in other types of crime know, once you pay, it makes you a potential easy target for future ransomware and other cyber-attacks. ❑

QR Codes and More

By John Krout, Writer/Presenter, Potomac Area Technology and Computer Society

Barcodes containing useful info now show up in videos and presentations. Learn how to use those barcodes.

www.patacs.org
krout75 (at) yahoo.com

A QR code is a square 2-dimensional barcode that provides useful info such as a web page address (URL). QR codes can also contain email addresses, contact info, and just about any text. It is not the only square barcode out there. QR codes can be recognized by the square target blocks in the top two and bottom left corners.

Illustration 1: pexels.com/video

Illustration 1 shows a QR code example. This particular QR code provides a web page address for a site where short user-created videos can be downloaded for free. You have probably seen square QR code barcodes many other times in recent years.

Illustration 2: Android 10 camera app reading QR code

My presentations for PATACS frequently include web page addresses. In this pandemic era of virtual meetings, I have decided to include not only the actual URL but also the QR code containing the URL.

Anyone in the audience who wants to copy the URL from the presentation immediately can do so simply by using their smartphone. Chances are that you won't even need to install a barcode reader app on your phone. In recent iPhones and Android 10 phones, the camera app has been augmented to act as a QR code reader.

I tried my Samsung Galaxy S10 camera app. I pointed it at the computer screen where a QR code was visible in one corner of a presentation. The camera app immediately displayed the web page URL contained in the QR code, as you can see in Illustration 2. I did not even have to snap a photo of the QR code. The app gave me the option of tapping the address to open that web page. Open-

Continued.....page 12

QR Codes.....from page 11

ing the web page is ideal for quickly saving the URL for later bookmarking.

Many retailers post QR codes enabling you to learn more about products.

MUNZEES

Illustration 3: Play Munzee URL

There is an outdoor game based on QR codes printed on small stickers posted outdoors. The name of the game is Munzees. I have not tried the game, though I know a few of my geocaching friends also play Munzees, and occasionally I see the small Munzees QR code stickers outdoors. Any small QR code in a place where it does not seem to identify any product or other specific object is quite possibly a Munzees QR code.

The Munzees game has its own website, www.playmunzee.com, and its own free phone app for communicating found Munzee QR codes to the website. That URL is encoded in Illustration 3.

CREATING QR CODESBy John Krout, Writer/Presenter, Potomac Area Technology and Computer Society

Illustration 4: QR code monkey URL

I found that my Galaxy 10 Contacts app will generate a QR code for any record in my Contacts list. When I create a contact QR code, it appears on the phone screen. At that point, I can save the QR code as a graphics image file, or attach it to an email or a text message.

There is a website, https://www.qrcode-monkey.com/, which creates QR codes containing the info you provide. It provides some interesting features, such as multi-color QR codes and placement of a recognizable logo in a QR code. You can download, save, print, and share any QR code you generate on that site. The site provides this service for free. That URL is encoded in Illustration 4.

OTHER TYPES OF BARCODES

There are several types of barcodes in wide use.

The Uniform Product Code (UPC) barcode on products, which enables rapid checkout and helps the retailer manage inventory, encodes information in several parallel vertical bars. That is an example of a 1-dimensional (1D) barcode. There are phone apps designed to scan UPC codes and tell you if the same product can be found for a lower price elsewhere.

If you have a driver's license, it contains both a 1D barcode and a 2-dimensional (2D) barcode. That 2D barcode is a type called PDF-417, and it includes all the text info on your license as well as some other info identifying your license record in the Virginia computer system. The American Association of Motor Vehicle Administrators (AAMVA) created a standard for contents of the driver's license

Illustration 5: AAMVA card standard URL

2D barcode and updates the standard everyfew years. That standard is available online as a PDF document. You can read the field definitions in section D.12.5 of the PDF posted at the following URL, which is encoded in Illustration 5.

https://www.aamva.org/aamva2020dlidcarddesign-standard/

The 2D barcode on the driver's license is now scanned by Safeway at checkout if you buy alcohol. That means the Safeway computer system may capture a great deal of info other than your date of birth. Does the company save all that additional info about you? Doing so centrally would use up a gigantic amount of storage space. Possibly the stores store the info locally, on a store server. That localized info could be valuable if a company store is audited by Virginia ABC for underage sales.

Barcodes also typically show up on shipment box labels.

United Parcel Service uses a 1D barcode type for machine-readable package tracking numbers. If you have received UPS parcels in person, you have probably seen the UPS driver use a barcode scanner to scan the tracking number barcode and confirm the date and time of delivery of the parcel.

While the phone camera apps will read only QR codes, other free apps can be used to read a variety of barcodes. I downloaded one Android with the rather generic name Barcode Scanner to read the Virginia driver's license barcode. The same app reads QR codes, UPC codes, PDF-417 codes, CODE 39 (1D barcode type, which appeared above the address in correspondence I received from the Arlington County Government), Data Matrix (another square 2D barcode type), and some other types. I used that app to read the PDF-417 barcode on my Virginia driver's license. ❑

ABOUT THE AUTHOR: John Krout has been writing about creative uses of personal computers since the early 1980s. Until April 2020 he was a software documentation writer, contracted to support a major federal government computer system.

SAFE EXPERIMENTING

By Dick Maybach, Brookdale Computer User Group

ww.bcug.com
n2nd (at) att.net

At the dawn of the personal computer age, life was simpler and more fun. Malware didn't exist, nor did the Internet, and the most valuable thing on our PC was the BASIC program Hunt the Wumpus. We continually tried new software (usually discarding it immediately). Now our PCs contain vital data, such as family photos, financial records, tax returns, and email history, which makes many reluctant to experiment. While the Internet is full of free and cheap software, much of it is tainted, and we are hesitant to take a chance with anything. Moreover, modern operating systems are complex, making tinkering with their organizations hazardous. As a result, we are sitting in a huge virtual library, but afraid to take a book off the shelf.

You can restore the adventure to PCs by setting up an environment, separate from the one presently on your machine, where you can experiment safely. However, remember that an effective backup discipline is always your last and best defense. Let's examine three such environments, virtual machines (VMs), dual-booting, and separate hardware.

No matter which environment you choose, you will need an operating system for it. If you use Windows, you have to purchase a separate copy, as the Microsoft license allows Windows to be installed in only one environment. Windows 10 is available (from Amazon) for as little as $50, which lets you achieve greatly increased security and yet stay in familiar surroundings. You also could use Linux, which opens up a whole new world of open-source software and which is generally malware-free, but the environment change

CONTINUED.....PAGE 14.

may be traumatic.

The easiest separate environment to set up is a virtual machine, such as Oracle's VirtualBox, but it requires competent hardware, at least eight Gbytes of RAM (16 is better), and 30 to 50 Gbytes of available disk space. When the VM is running, your hardware is supporting two environments, the one on your PC (called the host) and the one on the VM (called the guest). As a result, the guest environment may be noticeably slow, but less so if your hardware supports virtual environments. The key features on the CPU are VT-x on Intel and AMD-V on AMD processors, and these are now common, even on laptops. Be sure to check your VM documentation, as these features may be disabled in your BIOS.

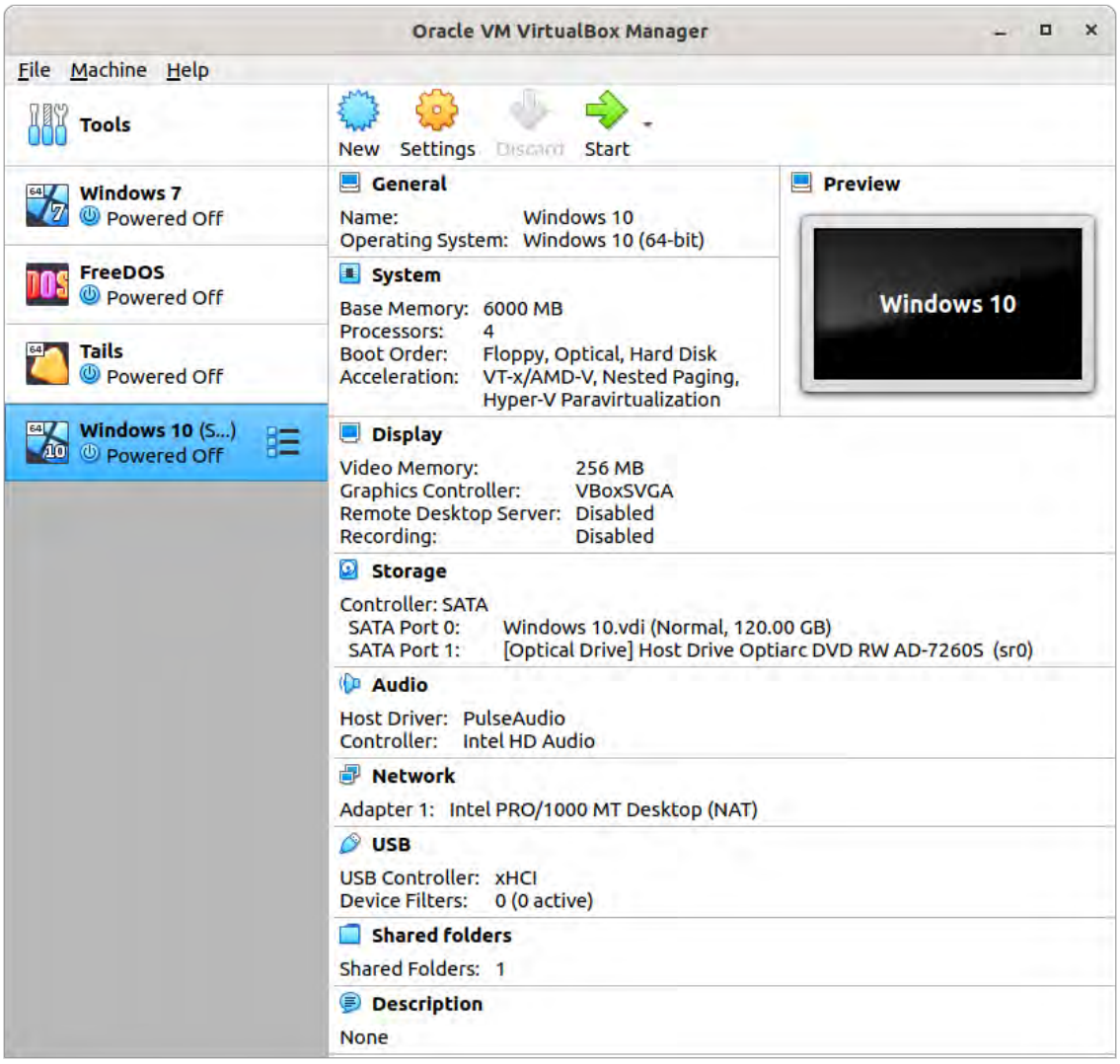


Figure 1. VirtualBox Manager.

In operation, a VM looks like an application to the host; see Figure 1, which shows the VirtualBox manager. You use a virtual manager to add, delete, and configure VMs, and this PC has four, Windows 7, FreeDOS, Tails, and Windows 10. The figure also shows a summary of the VM running Windows 10.

The VM snapshot feature is useful for experimenters. Making a snapshot is equivalent to cloning the

environment, and if the current experiment isn't successful, you can restore things with a click or two. Also, since VMs are just files on the host when you back up the host, you also back up the VMs.

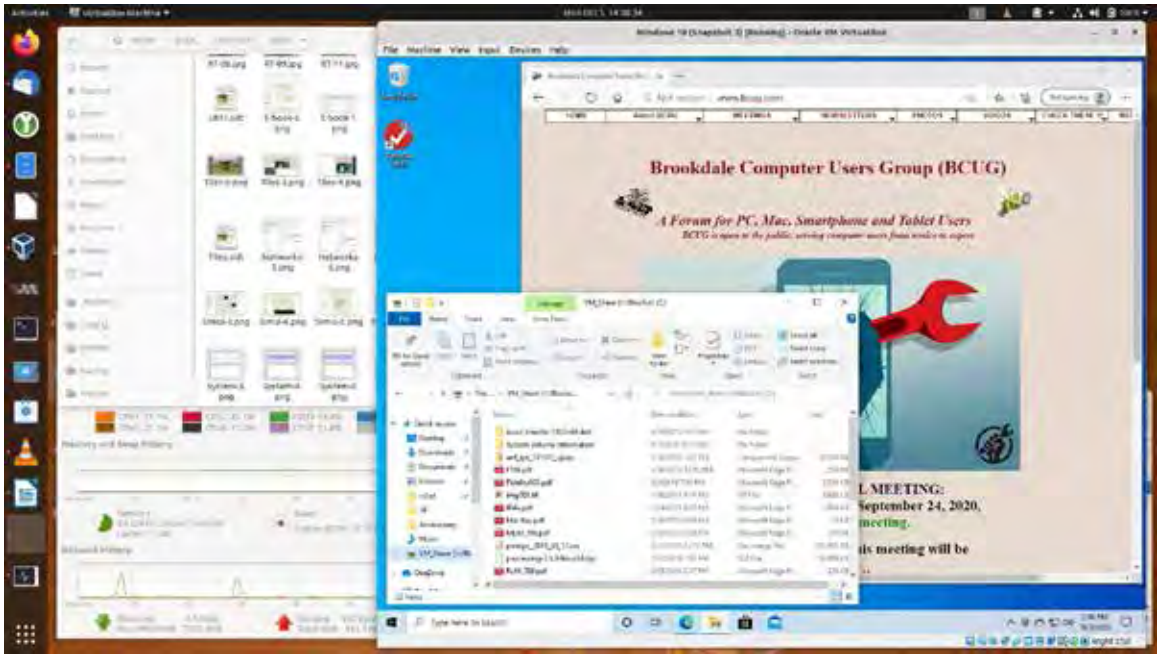


Figure 2. Host Desktop with a VM Running.

Figure 2 shows Windows 10 running in a VM on a Linux host. As you can see Windows has access to the Internet. Note also the file-manager window, which is looking at a directory on the host. Both Linux and Windows can access files in this directory, making it easy for the two to exchange information. You can also copy and paste between the two. However, these features require that you install the Guest Extensions to VirtualBox (see its documentation).

Before VMs became available, I used dual-booting for experimenting. This has the advantage of making all the resources of the host machine available to both environments; using VMs of course means that resources are shared between the host and the guest. The drawback is that setting up dual-booting requires some expertise and adds some risk. Here are the steps.

- Back up the system.
- Defrag the operating system to ensure that nothing is stored at the high addresses.
- Shrink the partition to make space for a second one above it. The second partition should contain at least 100 Gbytes. If you are short of space on your disk, you'll have to install a second one.
- Install the second OS in the second partition.

This involves more risk than installing an application, so do your homework before attempting it. You also must be careful to back up the second environment separately.

Continued.....page 16

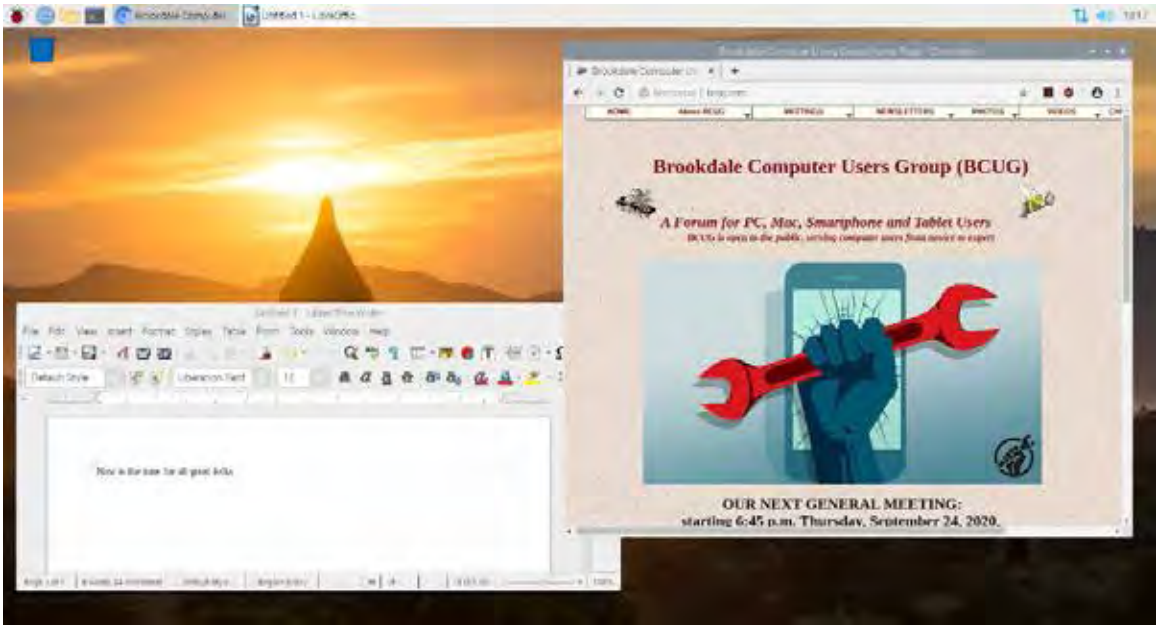


Figure 3. Raspberry Pi Desktop.

The last and safest method of obtaining a test environment is to use a separate PC. Many of us have old, unused machines, making this approach very cheap indeed. Its main disadvantage is the space occupied. If you don't have an unused PC or are short on space, consider a Raspberry Pi; it is model 4 that has as much power as a PC of not that many years ago; see Figure 3. If you share your PC display, keyboard, and mouse with the Raspberry, it uses almost no space. A KVM (Keyboard Video, Mouse) switch will allow you to do the sharing conveniently. Alternatively, you can set up a remote desktop to access the Pi from your PC, making the former appear as an application on the latter. It doesn't even have to be in the same room; all both need is a connection to your home network. If you haven't used a Raspberry Pi, you should first read the introductory material on its website, https://www.raspberrypi.org/. Setting one up is quite different than getting started with a new PC. Instead of a hard disk, it uses a microSD card, which you'll buy separately and on which you must install the operating system that you'll download from the Raspberry Pi website. The OS is a Linux variant, which probably involves yet more study, but the whole idea of experimenting is to learn.

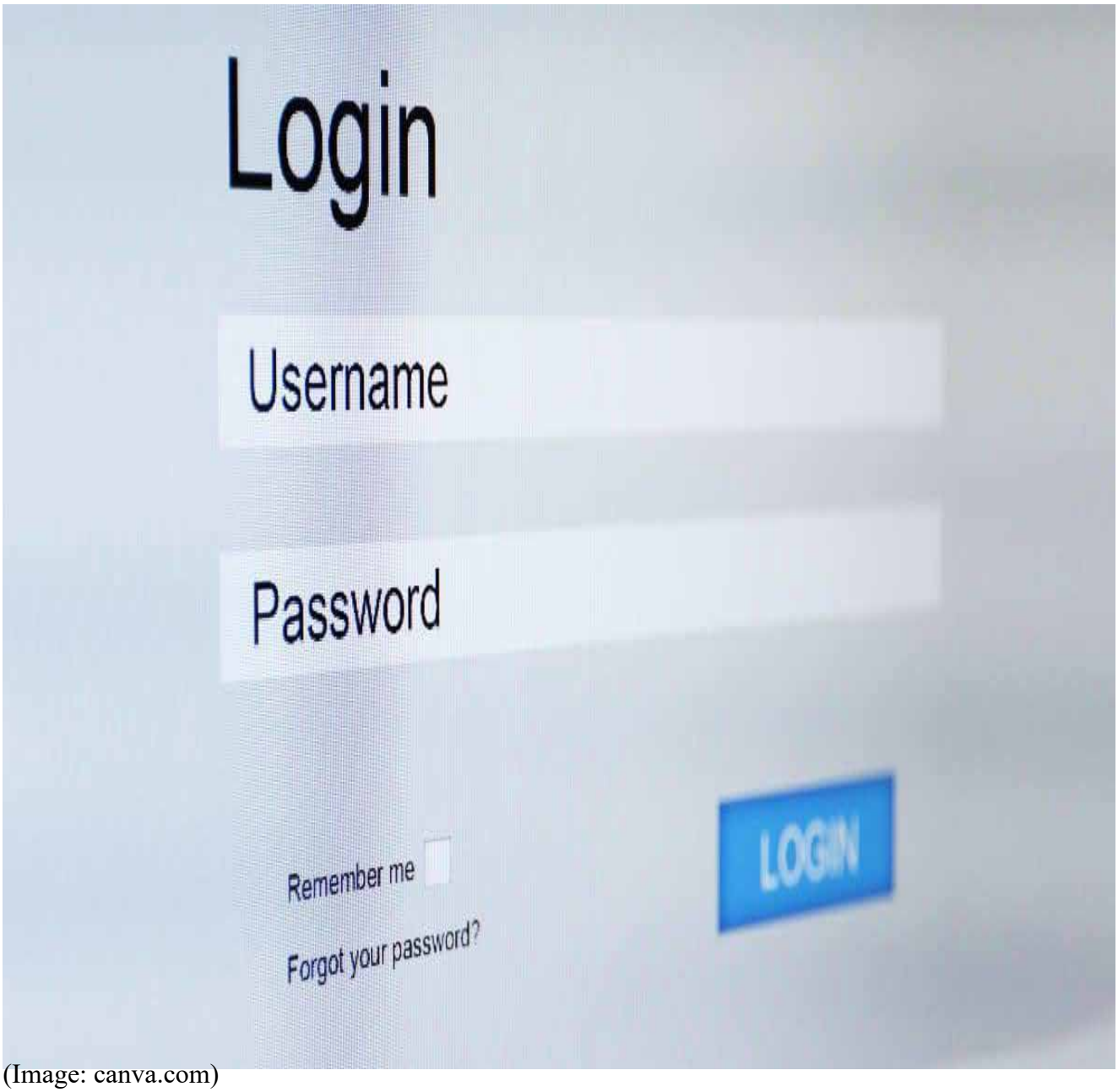
Once you have hardware for your test environment, you'll need an operating system. A VM and dual-booting give you the most flexibility, as you can use anything your host PC supports. With a Raspberry Pi, you'll be running Linux. Your options on a second PC depend on its age; older units may not support Windows 10 for example. You might also consider switching to Linux, as many distributions support older hardware. It also has thousands of free applications available.

Regardless of how you choose to do your experimenting, continue to exercise care if you transfer files to your home PC, as they can carry malware. Also, when you use virtual machines and dual-booting, you are not completely isolated from your home environment. Cross-contamination, while unlikely, is not impossible. ❑

ASK LEO

by Leo A. Notenboom

A One-step Way to Lose Your Account Forever
AKA: What not to do



(Image: canva.com)

I see people lose access to their most important accounts all the time. It's often their own fault that they can't regain access.

Not a day goes by I don't hear from someone who's in the middle of some kind of account recovery process that isn't working.

Continued.....page 18

Ask Leo..... from page 17

While I try to help out to the degree that I can — usually with instructions that are often no more than the service provider's instructions translated into clearer English — it's also not at all uncommon for those account recovery efforts to fail, and access to the account never be regained.

Never.

And to be super blunt about it, most of the time it's the account owner's own fault.

Account recovery fails most often because recovery information like alternate email addresses and phone numbers were never configured, or weren't kept up to date. It's important to set them and review them regularly to make sure they'll be there if and when you need them

The most common reason account recovery fails

Almost every online service has provisions for recovering lost passwords or regaining access to accounts that are inaccessible to their rightful owners. Those account recovery processes typically involve sending an email to an email address, a text message to a phone, or something else.

Those are great, reliable ways to prove you are the rightful owner of the account and should be allowed back in. Anything less would allow hackers to impersonate you or otherwise scam the system to break into accounts where they have no business being.

The problem?

Many people don't set up this recovery information, and those that do often don't keep their information current.

Without it, there's really no hope for recovery.

Alternate email addresses

These days, you should never have just a single email address.

You need at least *two*.
One you consider to be your real or primary address. The second can be configured as your "alternate" email address for that primary account. It is used should you ever need to prove that you are you.

Like, perhaps, when you forget your password …

… or when your account is hacked.

How do you prove that you are you? By being able to access that second email account. Account recovery frequently involves sending a password-reset link, code, or some other kind of information to that other email address. When you collect the information and use it, you prove you have access to that account. Since you're the one who set it up as the alternate account, then you must be who you say you are, and thus you should be allowed back into the account.

Never set up an alternate email address? You can't recover.

Lost access to the alternate email account? You can't recover.

The conundrum of the phone

Many services now allow you to associate a phone number with your account.

Unduly paranoid folks believe this amounts to more ways for the service in question to keep tabs on them.

I disagree.

Phone numbers are another way to prove you are who you are. Rather than sending you an email, these services can send you a text message with a recovery code, or in some cases, a recorded voice to read that recovery code to you. Your ability to receive a code at the phone number you provided proves that you must be you, and once again should be allowed back into the account.

The conundrum I allude to is twofold:

- Many services only support text messaging, and thus mobile phones. You'll need to use a different alternative authentication mechanism — like that alternate email account — if you don't have a mobile phone.
- This typically fails if you lose access to your account or are asked for additional validation while traveling outside your own country. Once again, make sure you have an alternate identification mechanism in place — like that alternate email address — before you leave.

Nonetheless, I do advise setting this up if you can.

Losing your account in one easy step

Pick whichever approach you like:

- Don't set up alternate authentication mechanisms like alternate email addresses or phone numbers at all.

or…

- Let your alternate authentication mechanisms expire, change, or lose access to them without updating the account for which they're the alternate mechanism.

Either works. You'll lose access to your primary account *forever* if you ever get hacked or lose your password.

Do this NOW

To avoid losing access to important accounts, I strongly recommend that you:

- Set up an alternate authentication mechanism on your important accounts.
- If you already have, go check they're all still valid.

Continued,,,,,,,,,,,,,,,,,,,,,,.....,,,,page 20

Ask Leo..... from page 19

I also recommend that you take advantage of all the alternate mechanisms offered.

- Set up an alternate email address, and keep that alternate email address active.
- Set up more than one alternate email address if you can.
- Associate a mobile phone number with the account.
- If you don't have a mobile, and the service will do voice calls (reading you a recovery code),
- then associate a landline number with the account.
-

And above all, any time any of the above changes, make absolutely certain to ***update the information*** in your accounts. Alternate email addresses or phone numbers do you no good if you no longer have access to them. ❑

The Windows 10 update mistake you're probably making

BY MELISSA HADAM, KOMANDO.COM

JUNE 23, 2021

Technology is constantly evolving, and there is a good chance that the computer you bought six months ago has already needed updates several times. Windows computers need to be updated regularly to work properly. **Tap or click here to find out how to update Windows the right way**.

You aren't alone if you are reading this and wondering what drivers are. In simple terms, a driver is just software that communicates with your computer, allowing it to operate properly. The bottom line, your drivers are important.

If you're set up for Windows 10 automatic updates, your drivers should be automatically kept up to date. There are some situations, though, when you'll want to update your drivers manually. This tip is brought to you by Dell.

When should you manually update your drivers?

Since your drivers should update automatically with software updates and updating manually isn't easy, this should be a last-case resort. In most cases, technical issues on your computer can be related to out-dated drivers. If you are experiencing any of the following issues, you may want to update manually:

- Your mouse isn't detected
- Monitor display issues

- An improperly-working webcam

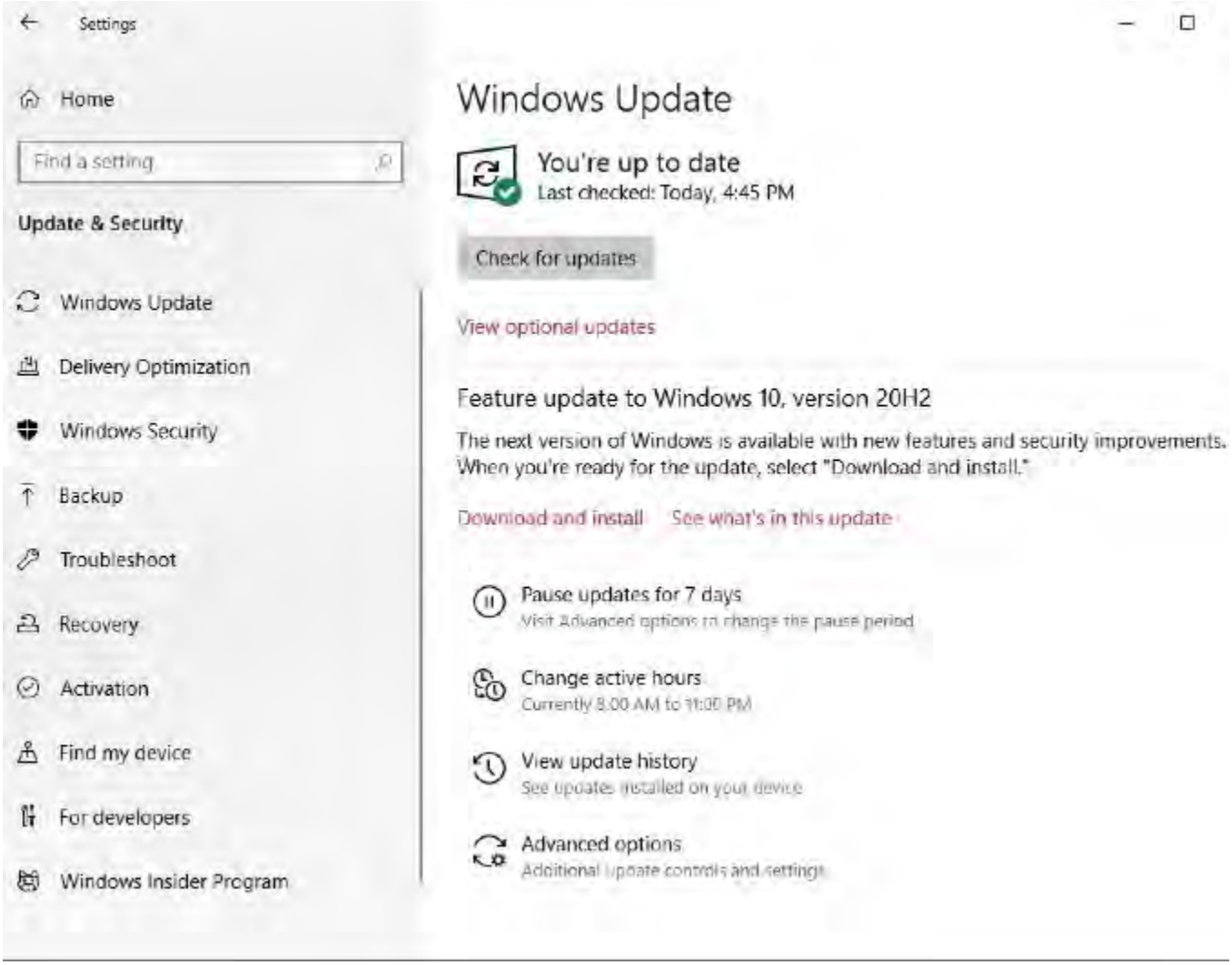
Before doing it manually, try double checking your updates

When it comes to messing around with the software on your computer, the less you do, the better. Ever mess around with your favorite cake recipe and end up with a hockey puck instead of a cake? Mistakes happen, especially when you attempt to be a computer expert, so try the automatic update first.

Bottom of Form

How to check for updates:

- Tap the **Start** menu button in the bottom left corner of your screen
- Select **Settings**
- Choose **Update and Security**
- Tap **Check for Updates**



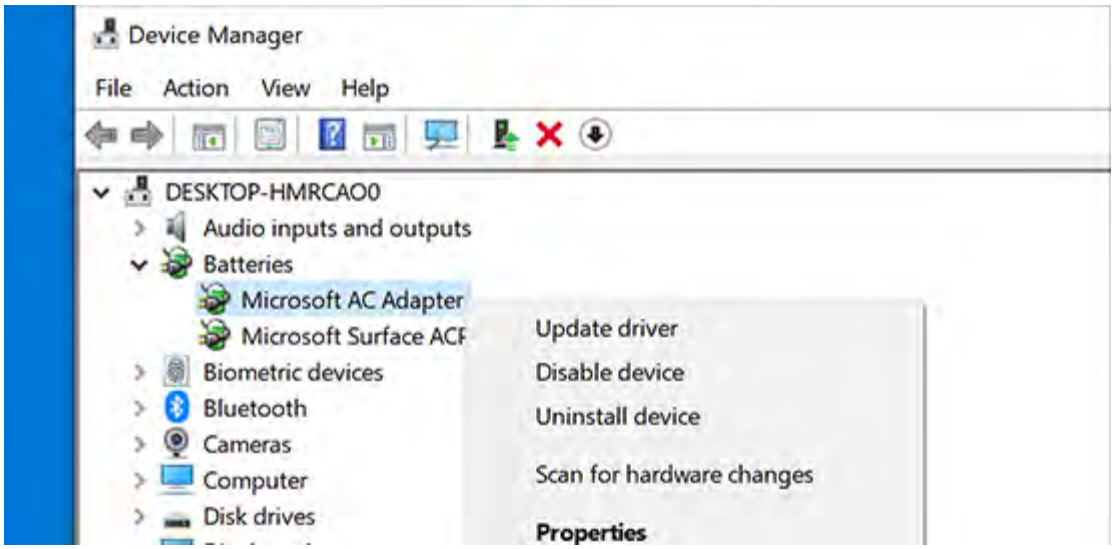
If there is an update available, select Download and install.

Windows 10 from page 21

Manually updating your drivers

If the automatic update doesn't work, it's time to update your drivers yourself manually. You'll have to update each category one by one manually. Here's how:

- Head to the **search box** on your taskbar
- Type **device manager**
- Select **Device Manager**
- Choose a device and right-click (**For example**: If you're having problems with your monitor, select monitor and right-click it)
- Tap **Update driver**
- Choose **Search automatically for drivers**
- If a driver update is available, update it (**Note**: If it already has the most recent driver, you'll see a message that says, "The best drivers for your device are already installed")



Not everyone is a technology whiz, but with these easy steps, you should be able to manually update your Windows 10 drivers. ❑

Print Nightmare is going to be a nightmare

by Susan Bradley

This is me.

This is me trying to figure out what best to do with a security issue in the news today. CVE-2021-1675 Or rather it's what I'd like to be doing but I can't.

So here's the deal. There's a security vulnerability for Print spooler that was patched back on June 8th but the patch didn't fully fix the issue. On June 21, the vuln was updated to critical severity as a potential for remote code execution was found. There is now a zero day proof of concept of this issue out on Github and various places. Specifically the proof of concept is for Windows Server 2019 but as I understand it, it impact more platforms as well.

Edit: Turns out this appears to be a new bug and not an unfixed vulnerability. Bottom line it's still just as bad but now just a regular old zero day instead of a slightly unfixed zero day. And it also works on Windows 11 as well.

Edit 7-2-2021 Micropatches from 0patch have been released for this issue

Action items if you are a consumer and DO print.

As I'm reading it, this is a big deal on domain controllers – not so much on stand alone computers.

Continued…….....page 24

Print Nightmare.....from page 23

This allows attackers to wiggle in via a remote authenticated user and raise the rights of that account. Since home computers do not have "remote authenticated users" I'm not freaking out here and recommending that you disable print spooler (yet). I don't know about you but I DO print so I cannot disable the print spooler service without severely impacting my productivity. I'll keep monitoring the situation and update if I see anything where I think consumers/home users/small peer to peer networks should be taking action other than the usual "be careful out here" and watch what you click on. So for now if you run windows and print, take no action, other than to be your normal, careful, slightly paranoid self.

Action items if you are a consumer and DON'T print.

Print spooler lately has been a big target. If you know you don't ever print or print to pdf or anything like that you can proactively click on the search box and type in "services", scroll down to print spooler, double click and click to change the service to stop and then to disable the startup type. Note you need to be an administrator (or have admin rights) to be able to stop this service.

Action items if you are a IT pro or MSP.

Determine if you can follow this post and disable the print spooler service especially on Servers, Domain controllers in particular. You might want to go through server hardening guidance while you are at it. Bottom line evaluate your risk for this attack and take action accordingly. Recommendation is to disable the print spooler service on the Domain controllers first. If you are a SMB consultant where your Domain controller is ALSO your Print server there's no good alternative especially if your folks have to print.

TrueSec have come out with a workaround that allows you to deny permissions to keep attackers from gaining system rights and leave print spooler service as is.

And if you are running Mint, Chromebook, Apple, etc. etc. just try not to look so smug, okay?
Print spooler lately has been a big target. If you know you don't ever print or print to pdf or anything like that you can proactively click on the search box and type in "services", scroll down to print spooler, double click and click to change the service to stop and then to disable the startup type. Note you need to be an administrator (or have admin rights) to be able to stop this service.

Action items if you are a IT pro or MSP.

Determine if you can follow this post and disable the print spooler service especially on Servers, Domain controllers in particular. You might want to go through server hardening guidance while you are at it. Bottom line evaluate your risk for this attack and take action accordingly. Recommendation is to disable the print spooler service on the Domain controllers first. If you are a SMB consultant where your Domain controller is ALSO your Print server there's no good alternative especially if your folks have to print.

TrueSec have come out with a workaround that allows you to deny permissions to keep attackers from gaining system rights and leave print spooler service as is.

And if you are running Mint, Chromebook, Apple, etc. etc. just try not to look so smug, okay? ❑

Windows 11 Compatibility Test Confuses Users

by John Lister

A surprise requirement for Windows 11 has left many users fearing their computer may not be compatible with the new system. The need for a Trusted Platform Module (TPM) has led to a price spike for the component, though there's no real need to panic or pay over the odds right now.

The requirement came to light when Microsoft published a downloadable PC Health Check tool that told users whether their PC met all the hardware requirements for running Windows 11, which is due for release later this year.

That led to a lot of confusion with users seeing the answer was "No," but the tool not saying where the problem was. Most of the requirements such as graphics card or minimum memory are fairly basic for modern computers so a lot of users will be baffled by the apparent failure.

Scalpers Cash In

The most likely explanation in many cases is that the computer doesn't have an installed and active Trusted Platform Module (TPM). That's a physical component that uses cryptographic keys for features such as encrypting entire hard drives or checking that a machine has the correct set of hardware and software during the boot process.

It seems Windows 11 will make a TPM mandatory as part of an overall effort to improve security on Windows computers. Specifically it›s looking for the 2.0 version of the TMP standard. (Source: theverge.com)

Some users have responded by rushing to buy a TPM that simply plugs in to the motherboard on their computer. Those normally cost around $20 but some sellers are now asking as much as $100 after a spike in demand.

Patience is a Virtue

For most users, this isn't necessary. The most likely explanation is not that their machine doesn't have a TPM, but rather that it hasn't been switched on. Doing so normally requires a change in the BIOS settings. How to access these settings depends on the specific computer but usually involves a key press that interrupts the boot process. (Source: windowscentral.com)
While that's simple enough for more confident users, most people shouldn't worry about it for the moment. It seems inconceivable Microsoft will launch Windows 11 while millions of users are either unable to install it or uncertain about the changes they need to make. The chances are that either Microsoft will ditch the requirement, or it will have to issue either an automated fix or extremely clear instructions for making any necessary changes.

Continued.....page26

Windows.....from page 25

There's also no real rush for Windows 11 as Microsoft will continue to support the latest editions of Windows 10 until at least 2025. In the unlikely event that TPMs really do prove a widespread barrier to Windows 11 upgrades and Windows 10 use remains widespread, that deadline might well be extended.

What's Your Opinion?

Have you run the PC Health Check tool yet to check for Windows 11 compatibility? Did you understand the results? Are you confident Microsoft will clear up the issue?

❑

Securing sensitive files in OneDrive's cloud

By Fred Langa

Does it feel like rolling the security dice when you save your files to a cloud-based service? When the files move out of your control and protection and into who-knows-what security measures the cloud-provider is using? You feelin' lucky?

It doesn't have to be a gamble. Here's how to take charge of your cloud-based file security to make your remote files snoop-proof and effectively just as safe as those on your local PC.

Plus: No, ProduKey isn't malware, despite what your security app says!

How to make files safe in OneDrive — or in any cloud!

AskWoody's recent OneDrive coverage from Lance Whitney, Susan Bradley, and me (see article list at end of this text) has unleashed a torrent of email from subscribers struggling with various aspects of OneDrive's poorly documented features and operations.

Questions about OneDrive's security are a common theme. For example, see this note from AskWoody subscriber Jimmy Dominguez:

> "Hi Fred! Could you provide us with your thoughts on the security of OneDrive? My main concern is putting my password app database on OneDrive. It's KeePass."

That's a great topic, Jimmy, and for much more than just password databases! You probably have many other private, sensitive files, too — financial records, tax information, health data, etc. — that you don't want to fall into the hands of cloud-based snoops.

The good news is that all major cloud-service vendors are extremely serious about the security of your data while it's in their care — the success of their cloud business depends on users' being able to trust

the service!

But your specific question was about OneDrive. Microsoft describes OneDrive's extensive security measures on the support page, How OneDrive safeguards your data in the cloud.

While that's all good — and truly, OneDrive's built-in security is good — it cannot be perfect. No human-built system ever is. Worse, it puts you (and your files) into a passive, subordinate position, totally dependent on someone else to correctly spec, implement, and maintain essential security for your cloud-based files.

There's a better way — easy steps you can take to ensure your data remains safe, no matter where it resides.

Let's start with Jimmy's password manager as the working example. It will lead us to a more general discussion of how to secure any type of cloud-based files.

First of all, yes, the KeePass password database is safe to sync to the cloud because, like all the major password-keepers I'm aware of, KeePass encrypts its database.

Today's high-quality file encryption is the very best way to add nearly impregnable security to any file, regardless of where it will be stored — in the cloud, on your PC, on a flash drive, in an email attachment, whatever. Without the correct decryption passphrase or password, the file contents will be safe and totally inaccessible.

A good password manager will also never transmit its data unencrypted, "in the clear." As you saw on the above-referenced Microsoft support page, OneDrive's cloud-based components automatically enforce the use of encrypted HTTPS connections anyway — so odds are no one will be able to snoop your data while it's in transit.

HTTPS adds good baseline security, but you can significantly enhance your online privacy by also using a VPN (virtual private network), which adds another, independent layer of encryption on top of HTTPS and can also disguise your physical location.

Many password-keeper apps also allow use of two-factor authentication when you first sign in, to verify that you're really you and not some snoop trying to break in. KeePass can use two-factor authentication, although it's a bit kludgy. See Tutorial — Using KeePass With Two-Factor Authentication.

And, if you employ OneDrive's Always leave on this device setting, as recommended in OneDrive's impermanent local copies (AskWoody Plus 2021-05-24), your working copy of the encrypted KeePass database will be kept local with a separate and still-encrypted copy tucked away in the Microsoft-protected cloud, synced there via encrypted HTTPS/VPN transmission. I'd say that's very, very safe!

OK, that's KeePass. But you can employ the same concepts to achieve similarly safe transmission and storage of all your sensitive cloud-stored files — financial records, tax information, health data, etc.

The bedrock concepts are to employ file- or folder-level encryption on the files/folders that will sync to the cloud; to use only encrypted communication (e.g., HTTPS and/or a VPN); and, if available, to use two-factor authentication when first signing in to your cloud-based apps and services.

Continued.....page 28

Securing Sensitive.....from page 27

Encryption can be easy and virtually automatic. For example, the MS Office apps offer optional, built-in, high-quality, 256-bit AES encryption (Microsoft calls it password protection; see Protect a document with a password.) Just save your Office files this way, using a good, un-guessable password, and your files will be effectively un-snoopable by anyone, anywhere.

If you use apps without built-in encryption, you can instead use a simple external file- and folder-level encryption app such as 7-Zip (open source/free; site). 7-Zip can encrypt virtually any file or folder.

Note: Whole-disk encryption does not work this way. Systems such as BitLocker encrypt files only while they're physically present on the local hard drive; the files lose their encryption when they're exported from a BitLocker-encrypted disk. To secure files in the cloud, you need a file- and folder-level encryption tool such as 7-Zip; not a whole-disk encryption tool like BitLocker.

As for communicating with the cloud, make sure your cloud provider enforces use of **HTTPS** connections. I strongly suggest that you use a reputable **VPN**.

Choosing a VPN can feel random because there are a million services available, free and paid, as this example Google VPN search shows. I'm not a VPN expert by any means, but to give you at least a known-acceptable starting place, my consumer-level experience with ExpressVPN has been positive. It's been fast and reliable for me from multiple locations, and it allows one VPN subscription to cover all my and my wife's digital devices — PC, Android, Linux, Chromebook, Mac, and iOS. It has a good reputation for security and comes with a 30-day, money-back guarantee. But, again, this is only my personal, anecdotal experience; there may be other VPNs out there that better suit your needs and preferences. Search away!

Bottom line: OneDrive is reliable and reasonably safe on its own. Add in **file- and folder-level encryption,** secure communication via **HTTPS and VPN**, and maybe **multi-factor authentication**, and your cloud-based files will be about as safe and secure as humanly possible!

Related info:

- Is the cloud unsafe? (AskWoody Plus 2021-05-10)
- Is your deleted cloud data really gone? (AskWoody Plus 2020-03-09)
- How to close that dangerous, semi-secret "back door"! (contains more information on file- and folder-level encryption; AskWoody Plus 2021-03-22)
- A cloud-storage skeptic weighs in (scroll down in AskWoody Plus 2021-03-22)
- Fundamentals of Cloud Service Reliability (Microsoft white paper)

More OneDrive coverage in recent issues:

- Microsoft OneDrive: The basics (AskWoody Plus 2021-02-01)
- Using Microsoft OneDrive on your Android device (AskWoody Plus 2021-03-01)
- Using OneDrive on your iPhone or iPad (AskWoody Plus 2021-02-15)
- OneDrive, several problems (AskWoody Plus 2021-04-19)
- More on OneDrive, and symlinks (AskWoody Plus 2021-05-03)
- Another OneDrive problem caused by poor documentation (AskWoody Plus 2021-05-17)
- OneDrive's impermanent local copies (AskWoody Plus 2021-05-24)
- All storage is not created equal (AskWoody Plus 2021-04-19)

Is ProduKey malware?
In Win7 to Win10 activation trouble (AskWoody Plus 2021-05-24), I mentioned ProduKey as a free example app that can dig out the product keys for Windows and other apps installed on your PC.

But some readers, including Bob Petruzzelli, encountered a snag:

> "Fred: Just to let you know I was reading your article this morning and tried to download the ProduKey app.
>
> "Windows Defender was adamant that it was a virus and wouldn't let me download it. I created a dummy **.zip** file and added it to the Windows Defender exclusions in my download folder. Then I could download it. But then when I unzipped it the **.exe** file was instantly deleted by Window
>
> Defender, whoosh…. So I made a dummy file for that in the Windows Defender exclusions\
>
> ""Then I could finally run the file and get my Product Key."

Thanks, Bob. ProduKey isn't a virus, of course, but many browsers and security apps see that it's trying to get at product keys, and they incorrectly assume that something evil must be happening.

But yes, with Windows Security (formerly "Windows Defender"), you'll usually have to click through several layers of warnings before the file safely arrives on your disk, and several more to get it to run.

It's confusing and a bit of a pain the first time you encounter this kind of adamant blockage by Windows Security, but the support information at Add an exclusion to Windows Security can help you get the file to run.
Alternatively, there are many other product key-finder apps out there (examples). Feel free to experiment until you find one that works the way you — and your anti-malware app! — want it to. ❑

B U G Officers

President

Bill Middleton

President@bugclub.org

Treasurer

Loretta Mills

Treasurer@bugclub.org

Secretary

Bill Middleton

Secretary@bugclub.org

Member At Large

Jim Townsend

Webmaster

Chris Crisafulli

Webmaster@bugclub.org

Special Interest Groups

Beginners' SIG:

beginners@bugclub.org

Hardware (Tinkers) SIG:

Bob Schmidt 952-0199

hardware@bugclub.org

BUG Web Page

http://bugclub.org

Brevard Users Group Secretary's Report

By Bill Middleton

One Senior Place Meeting - Monday, May 10, 2021

1. The meeting was called to order by President, Bill Middleton at 2:00 PM.
2. Members were urged to pay their dues and make sure their registration details were up to date. Dues may be paid at any meeting or mailed to the BUG Club, PO Box 2456, Melbourne, FL 32901. Please make sure your current email is included with any mailed-in dues.
3. The Month's DD was on tablet computers. The iPad is generally acknowledged as the best of these little gadgets. The competition devices are generally powered by Google's Android operating system or a modified version of it. Microsoft ported Windows to the tablet world but it wasn't very well received. They pouted a bit and applied the technology to their high-end Surface devices which are basically small, expensive, full-fledged computers with a removable display that can be used as a tablet. Samsung's Galaxy Tabs are the high-end in the Android world and are quite expensive. For those of us of modest means, there are the pure Android tablets such as Walmart's RCA line and a number of Chinese-based brands sold by

other retailers and mail-order outfits like Wish.com and Aliexpress.com. The president considered the best performing and most cost-effective Android-based devices are those supplied by Amazon. The performance of the eight and 10 inch devices is damn close to iPads' and

they sell for under $150 ($100 on Prime Day and other Sale days). To get the most out of them, you should also sell a piece of your soul to Jeff Bezos and sign up for Amazon Prime. If you want to make your tablet more like a regular computer, you can buy a Bluetooth keyboard. And Microsoft will now sell (or rent) you Office for Android. Silk Purse, anyone?.....

Of the few tablet users present, no one expressed interest in adding a keyboard or Office.

4. Subsequent discussions are mainly about cell phone issues.
5. The meeting was adjourned shortly after 3:00. The Financial SIG followed.
6. Respectfully submitted by Bill Middleton, Secretary. ❑

Bug Club Treasurers Report
By Loretta Mills , Treasurer

Checking Account	**July 1, 2019**
Beginning Balance	$ 1052.36
Ending Balance	$ 1052.36
Saving Account Balance	$ 1087 65
Combined Balances	$ 2140.00

"Windows Event" on the 24th which is the subject of this month's DD: WINDOWS11???! We'll explore the online speculation and throw in our own two cents or more. Should be fun speculation and we'll only have to wait a week and three days to find out THE TRUTH! For our cell phone & tablet folks, we'll talk a bit about Android 12, which just went Beta (will Bill's new car demand he get yet another new phone?). Q&A will follow.

Note: It is expected that the Covid restrictions in the Libraries will be eased in July, but there is no word on when the Fee Ave Library's large conference room will again be available, so we'll remain in the small one for now, but we'll be allowed more attendees.

General Meeting Notice

It's time for our June General Meeting at the Eau Gallie Library on Monday June 14 at the usual 2:00 PM. Covid restrictions still apply at the Libraries so bring a mask. Come, help decide whether to put the remains of our Treasury into Bitcoin or Dogecoin (Doggycoin?). After Prime Day (JUNE 21/22), will come a

"I've been promoted to Executive Director of Personal Energy Management Resources. I'm in charge of coffee and doughnuts."

Going North for the summer or coming back?
Don't miss a single issue of your

Space Coast PC Journal

If your email address will be different

Please give us the correct email

For your temporary location

*****Reminder*****
We need your e-mail addresses!
We'd like to keep in touch with you, especially if there is a last minute change in venue for the club meeting.
Please send e-mail addresses and changes to
Linda Glassburn glassburn@earthlink.net

Are you having problems with your hardware or software?
Did you find the solution yourself?

How about sharing that information with your fellow club members? Sit down for a few minutes open up that word processor and put your ideas to paper. Aside from the value to the members, you'll get your name in print!

Don't worry about the details, we'll edit it for the best appearance and presentation.

Calendar of Events

Club Meeting, 2 PM July 15
Auditorium, Merritt Island Library

July 31, 2021 - Deadline for Journal Input

Presentations Schedule

Bring Some Friends or Neighbors

Beginners or Advanced
Bring Your Questions
Get Technical Help
Share Your Knowledge

at Your SCPCUG

Learning Center

Open 1st, 3rd, 5th Saturdays,
12 to 3:30 p.m.
Merritt Island Library
Conference Room

Please restrict your visits to these times.

Bring your hardware or software problems,
We'll do all we can to help.

If you bring a desktop computer please bring the keyboard, mouse, and power cord

Call Ron Ingraham, 321-777-2578, for more information.

The
Space Coast PC Users Group Journal

is produced using

Adobe InDesign CS3

All SCPCUG club members are entitled to receive the electronic version of the Journal in pdf format. You'll need Adobe's widely available Acrobat Reader X.X (free) to view the eJournal.

Contact Ron Ingraham
ringram28@cfl,rr,com to get on the eJournal mailing list

Space Coast PC Users Group is proud to be a Charter

Member of
Association of Personal Computer User Groups
APCUG

The Space Coast PC Users Group's

Computer Doctors

Make House Calls

***Free* to**

SCPCUG Members!

Dan Douglas, owner of
DataDan Computer Services,
will accept phone requests
for computer assistance
(321) 301-1075
After a phone call, a house call may be made within 5 miles of Merritt Island

Free Remote Support
For those using Windows 10
Quick Assist

The above member will help you with ***a particular*** computer glitch on your personal (not business) computer. In some cases, he may even make a house call. But, please do not expect him to install your computer nor teach you how to use it. If you have continuing problems or need additional help, please take a class, or check the ads in the *Journal* and hire a consultant, etc.

Computers 4 Kids

C4K Volunteers Need Donated

Computers, Keyboards, Mice etc

for

Building PC Systems

complete with software for

Needy School Children

Call

Ken Clark @ 223-7402

To arrange pickup

Space Coast PC Users Group, Inc.
MEMBERSHIP APPLICATION

Membership Dues
$25.00 [ ] Check [ ] Cash

Check No. _____

NAME _____ [ ] New [ ] Renewal

ADDRESS _____ Date _____

CITY _____ STATE _____ ZIP _____

Home Phone _____ Work Phone (Optional) _____

E-mail _____

Would you like to attend: a class for BEGINNERS? [ ]
an ADVANCED DOS class? [ ]
a WINDOWS class? [ ]
an ADVANCED WINDOWS class? [ ]

What other topics would you like covered in a class? _____

Do you have expertise that you would like to share? Please describe.
_____ ☐

Would you be willing to be listed in the Helpline of the *Journal*?
If so, what subject? _____ Calling hours: _____
Phone _____ E-mail _____

Would you like to help the Club in the following areas?
Resource Center Staff _____ Journal Staff _____
Computer Doctor _____ Room Setup _____ Teach Class _____
Other _____

What topics would you like to see for monthly programs?

What can the SCPCUG do to help you and others?

If you were told about the SCPCUG by a club member, write that member's name here _____

DRAM CPU **Are You Bewildered?** HTML Windows Modem

Join the
Space Coast PC Users Group
and learn the lingo!

Membership benefits:
- The *SCPCUG Journal*
- Computer Literacy Classes (e.g. Windows 7-10)
- Seminars and Workshops
- Computer Doctors - computer help - **FREE**!
- Group Purchases, Raffles, and Door Prizes!
- Helplines - get help from the experts

Join Now!

Make check payable to: Space Coast PC Users Group

Mail to: SCPCUG , 801 Del Rio Way, #304, Merritt Island, Fl 32953

ADVERTISING RATES

SIZE	1 Month	3 Months ~10%*	6 Months ~15%*	1 Year ~25%*
Full Page	$90.00	$243.00*	$459.00*	$810.00*
Half Page	45.00	123.00*	230.00*	405.00*
1/4 Page	23.00	62.00*	117.00*	207.00*
Business Card	35.00	59.00*	105.00*	

* = Discount from regular monthly rate. Discount applies to ads running in consecutive issues.

Payment **must** accompany order. Make checks payable to:

Dimensions (W x H) for ads are as follows:

Full page:	7" x 9 1/4"
Half page:	7" x 4 3/8" or 3 3/8" x 9 1/4"
Quarter page:	3 3/8" x 4 3/8"
Business card:	3 3/8" x 2"

Camera ready ad copy is due by the 28th of the month to ensure that the ad will appear in the next issue. Mail ad copy to the Editor at1360 Mayflower Avenue, Melbourne, Fl 32940-6723 Prices will be quoted for design work. Questions? Call (321)777-2578.
All advertisements are subject to the approval of the Editor.

SPACE COAST PC USERS GROUP, INC.
801 Del Rio Way, #304,
Merritt Island, Fl , 32953

STATEMENT OF PURPOSE

The Space Coast PC Users Group is an independent, not for profit, computer group open to anyone interested in computers. It is not affiliated with any business. Our purpose is to serve as an educational, scientific, and literary organization designed to enhance computer literacy.

DISCLAIMER: Neither the Space Coast PC Users Group, Inc. (SCPCUG), its officers, board of directors, nor members make any expressed or implied warranties of any kind with regard to any information or offers disseminated in the *Journal* via advertisements or articles, including but not limited to warranties of merchantability and/or fitness for a particular purpose. Opinions provided by *Journal* articles, or by speakers, members, or guests who address the SCPCUG meetings are individual opinions only, and do not represent the opinions of the SCPCUG, its officers, the board of directors, or members. All opinions, information, and advertisements should be carefully considered by every individual and neither the group, its officers, board of directors, nor members shall in any respect be held responsible for nor be liable for any and all incidental or consequential damages in connection with or arising out of the furnishing or use of any information, advertisements, or opinions provided by or through the Space Coast PC Users Group.

Initial Membership $25 . Annual Dues have Been Suspended

BENEFITS: Members get the monthly *Journal*. In addition, ***only*** members can:
· copy from the Shareware library
· participate in meeting drawings
attend special seminars/workshops
talk to one of our computer 'doctors'
· use the Helplines

NEXT MEETING
July 15, 2021

Merritt Island Library Auditorium 1185 North Courtenay Parkway,
Merritt Island, FL

Guests are always welcome at the Space Coast PC Users Group meeting.