The Space Coast PC Journal

HAPPY NEW YEAR!!

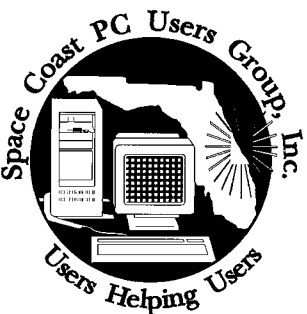## Still Another one -----------gone

Here's hoping that **2020** will bring
the changes that some of us so
desperately need.
Wishing you and yours
a Healthy, Happy and Prosperous
New Year!!

from your Board of Directors

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

Visit Our web Site at www.scpcug.com

All work on the Journal is performed by unpaid volunteers.

From The Editor

Here we are in the New Year. I fear that it will be more of the same as far as this group goes. I don't see any drastic changes any time soon. We're really very fortunate compared to many of the other groups around the country, even arond the world.

One example caught my attention as I was looking for articles. The Green Valley Resort Computer Club, AZ had submitted an article from their publication , the April-August 2019 issue. They're not the only one I've run across that only publish every three or six months. Granted Green Valley is a resort and the cited 6 months are their hottest. Maybe most of them head for cooler climes.

However, it became apparent to me while reading Newsletters for the contest , that many of them are on the verge of shutting down because of reduced membership or loss of interest

We see some of this in the declining attendance at both the Learning Center and the monthly meeting. It is apparent that this Journal seems to be what is keeping most of our members with us. Unfortunately it's becoming harder every month to find articles to include. You may notice that I've had to resort to going back as much as a year to find articles from Judy"s PUSH that I hadn't used when I received them.

Fewer Group members are writing and many groups are filling their newsletters with identical articles for lack of a reliable source. I am having the same problem. I'll keep plugging, though.

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

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.   ❑

*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 ....Harry Pearson   harrymp@cfl.rr.com 868-1814
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......................338-5414
                                   yjm1938@yahoo.com.

.

Professional also includes DriveScrubber, a utility that can securely

**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
January 16, 2019

The monthly meeting will
be an informal question
and answer session.
Bring your problems
Someone should be
able to help.

Bring Some Friends

On Guard! Top Scams Point to Need to Monitor Your Card Accounts

By Scambuster Keith,   SCAMBUSTERS Newsletter
December 25, 2019

As we move into the third decade of the 21st century, it's a sad fact that Internet scams have become a part of everyday life.

A crime that was barely known at the beginning of the century has reached a point where, according to a new survey, 9 out of 10 of us say we've been victims of a scam.

The survey of 2,000 people, published just a couple of weeks ago by cash-wiring service MoneyGram, cites online scams, fraud, data breaches, identity theft and social media hacking as the main sources of scams.

The most common online scams were romance/dating cheats and various tricks designed to get victims to wire money or gift cards after being threatened by imposters claiming to be police, tax and court officials, or by falling for tech-support, coercion and blackmail scams.

Scambusters' tracking of crime reports and other anecdotal information suggests that romance scams in particular have been one of the major crime growth areas during the past 12 months.

Not only that, but statistics suggest that victims are parting with huge sums -- $250,000 in one case -- by falling for supposed lovers' sob stories. The scammer, having spent months or years grooming their victims, suddenly asks for financial help.

Often, the victims are middle aged or older women, some of whom admit they've handed over their entire life savings after falling for a scammer's lies.

Fake websites designed to look like the real thing and phony tech support callers account for a large share of identity theft scams. However, as we know from the news reports we get every day, the major sources of ID theft are data breaches at big name firms.

These were up 50% during 2019, with more than 3,800 incidents reported in the first nine months of the year.

All things considered, it's surprising that 10 out of 10 of us didn't report being scammed!

No Wiser

What is worrying, as we move into the New Year, is the number of consumers who still have not wised up to some of the scammers' most obvious tricks.

For example, the MoneyGram survey showed that less than half of respondents knew that being asked to wire money to a stranger was a glaring danger sign. Only about the same proportions were wary about get-rich-quick offers and threats of jail if they didn't pay a non-existent penalty.

That suggests that the other half of the population are open to these scams. In fact, alarmingly, 10 to 12 percent of the people polled admitted they'd answer an email from an unknown source, respond to romantic requests online or to a job offer they'd never applied for. And a third of the respondents said they didn't take any type of precautions to protect themselves while shopping online.

There's obviously still a big education job to be done.

As MoneyGram chief operating officer Kamila Chytil says: "Increased internet usage, sharing our lives on social media and the growth of non-face-to-face interactions are just a few factors that put consumers at risk and make it more important for financial services providers to help protect and educate our customers."

Given all of this, it's highly likely that confidential details of every single one of us who use the Internet have been compromised in some way. Somewhere, someone has that information -- whether it be bank account or credit card details, email addresses, Social Security numbers or other data we'd rather others didn't know.

We can't stop them. So, as we move into the next decade, it's going to become increasingly important to monitor credit card and bank accounts on a daily basis. While we may not be able to keep our information out of the scammers' hands, we can stop them using it.

From the Cashier's Cage

Financial Report for Month
Ending December 31, 2019

CHECKING

Beginning Balance	December 1, 2019	671.46
Barbara Mead – September snacks		(10.00)
Snack fund – November donations		7.00

Ending Balance - December 31, 2019
Includes $180.80 Snack Fund   668.46

SAVINGS

Beginning Balance December 1,2019	404.72
Interest	.09
Ending Balance	404.81

Total Account Balance December 31, 2019 1073.27

And if you can't check accounts daily, consider using a third party to monitor your records with the credit reporting agencies. There are paid and free services. If you don't know where to start, check out this report: https://www.thebalance.com/best-credit-monitoring-services-4164937

More of the Same

Beyond this, we see most of 2019's top scams continuing through 2020, notably those romance and imposter tricks.

Furthermore, as we have already reported, with 2020 being an election year, we're likely to see a surge in fake news and photos. In particular, the growth in what are called "deep fakes" -- videos that have been doctored to make someone appear to be saying something scandalous that they didn't really say -- will be evident.

No matter what your political leanings, we urge you to be skeptical about sensational stories and to check them before forwarding them.

In 2020, the age of Internet honesty, if it was ever here, is over. Security software companies are battling the scammers to protect us, and lawmakers are scrambling alongside them.

But unless we take responsibility and educate ourselves about the risks and the top scams -- and encourage friends and relatives to do the same -- we will remain firmly in the sights of the scammers.

Alert of the Week

Payments processor Visa has issued an urgent warning about malware at gas stations -- both at the pump and inside their convenience stores.

Crooks have been hacking their networks to get access to point-of-sale (POS) equipment -- devices used for reading debit and credit cards -- that still use magnetic strips instead of chip readers.

There's nothing you can do about it. It's the business owners' responsibility to take security precautions and you have no way of knowing if they have.

The safest action is to pay with cash. But if you do use your card, make sure you check your statements regularly for signs of fraud.

That's it for today -- we hope you enjoy your week! ❑

"It probably violates child labor laws, but we needed someone with hacking skills."

Dan's Desk

I want to start off the new year by expressing my deep felt gratitude to all of the board members and other volunteers that make the SCPCUG such a fun, entertaining and always an educational experience for all of our members. Irene for keeping our accounts up to date; Linda for keeping our membership records accurate and recording the attendance at each event; Larry for scheduling speakers in a world where everyone is used to meeting online and not in person; Harry for keeping our meeting records and keeping us on track; Barb for the lovely treats she serves at the meetings (and never forgets my Diet Coke!); Curt for maintaining our communication to the online world and publicizing our events with words and pictures; Ron for crafting a masterpiece of a newsletter every single month in a time when most clubs and groups have been reduced to an occasional single page letter.

When Larry approached me in 2012 to first speak to the group and then when Harry asked me if I'd be willing to serve on the board, I had no idea that it would lead to some of the best relationships and great opportunities in this stage of my life. So I thank all of you for keeping the SCPCUG going.

Although we have been successful in adding new members last year, we may need to revisit our annual membership dues policy. We have now gone several years with suspending the previous policy of charging an annual fee of $25, primarily because we had such a substantial bank account balance built-up. But Christmas parties cost money, so we may have to consider adding an event charge or going to some sort of annual fee again. Please let me or the other board members know what you think would work best for you.

Please have a great 2020 and I look forward to seeing you at our monthly meetings and helping you solve problems and socialize at the Learning Center Saturday events.

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

Very Large Array (VLA)

Author: George Harding, Treasurer, Tucson Computer Society, AZ

July 2019

www.aztcs.org
actuary110 (at) yahoo.com

The VLA is a physical structure about 50 mile west of Socorro, New Mexico. It consists of 27 large disk radio telescopes in a "Y" arrangement, a Control Center and various auxiliary structures. The purpose is to capture and analyze radio waves being emitted from space to create meaningful pictures and data about outer space objects.

It was originally created in 1980 and has been significantly improved since then. It is used by astronomers and others as needed in their respective occupations.
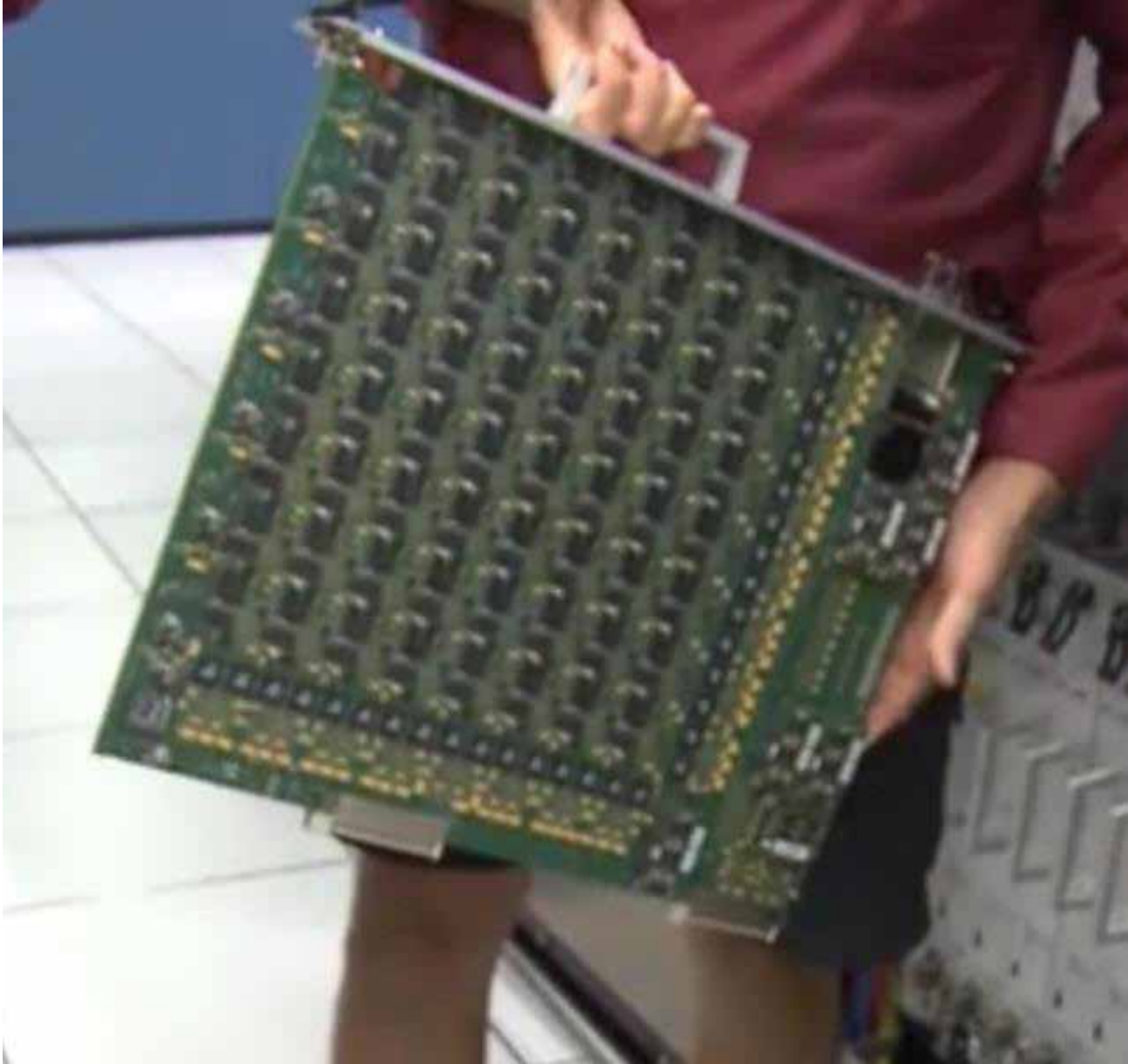

Each disk is massive, weighing 220 tons and is 82 feet in diameter and 94 feet high. It can rotate and tilt so as to aim in any given direction. Any disk can be moved along special railroad tracks. Since each disk presents such a large surface, they are subject to damage in high winds. In this event, the disk is parked pointing upward to present the least surface for the wind.

Each leg of the "y" formation contains nine disks, which can be rearranged in several ways. The configuration changes periodically from fully spread out along the "Y" to fully compressed and to two intermediate designs. The effect is to widen the aperture of the telescopes or to narrow them.

The signals from each disk are transferred by fiber optic cables to a system which translates the analog data to digital. The process is quite complicated but is performed by a supercomputer called the correlator.

Each of the boards comprising the correlator contains some 180 ICs each with from 250 to 600 pins. VLA personnel state that it is five times faster than the fastest general- purpose computer in the world!

Anyone can access the data produced, for whatever purpose desired. The VLA can be requested for a particular job needed by an astronomer by submitting a proposal. If approved, the proposal is translated into a script for controlling the array for a specific period of

time. After completion, the results are given to the requestor and after some months made available to the general public.

The facility is open to the public and a visitor center is available. Tours are provided from time to time.

The site of the VLA is the plains of San Augustin, selected to be as far away from other electronic emanations as possible. Cell phones, for example, emit a radio signal several hundred times louder than the faint signals from outer space. Visitors are asked to keep their phones in airplane mode to mask these signals. In addition, the plains are surrounded by mountains which help to shield the array from man-made radio noise.

For more information see
https://public.nrao.edu/telescopes/vla/

The Very Large Array is owned and operated by the National Radio Astronomy Observatory. ❑

Report: Most Facial Recognition Software 'Racist'

by John Lister on December, 26, 2019

From Infopackets Newsletter
Infopackets.com

Facial recognition software may be less accurate when dealing with non-Caucasian faces, according to a new study. The National Institute of Standards and Technology (NIST) noted the problem was likely the data used to «train» algorithms.

The NIST examined 189 algorithms from 99 different developers, which it says is a majority of all commercially available systems. (Source: bbc.co.uk)

In the testing, it looked at two tasks. Specifically, they looks to see if two specific photographs are of the same person. In one example, it was to verify identity in order to unlock a phone or check a passport; the second was to spot any match between one photo and an entire database - for example, when reviewing live video footage to spot anyone who is a ‹person of interest›.

Results Vary Across Globe

The study looked for two errors: false positives, where an algorithm wrongly says two pictures are of the same person; and false negatives, where an algorithm fails to spot that two pictures are of the same person.
Overall, the algorithms tested were more likely to give a false positive for Asian or African American faces compared with Caucasian faces when comparing two photographs. That could mean, for example, that facial recognition unlocks were less secure for non-Caucasian faces. With some algorithms, the error rate was 100 times greater for non-Caucasians.

The effect varied depending on the country where the algorithm was developed. For US algorithms, the results were less reliable for non-Caucasians, with particularly low accuracy for American Indians. For algorithms from Asian countries, there was no significant difference between accuracy among Asian and Caucasian faces. That could mean the problem isn't the algorithm as such, but rather the database of photos used to develop it.

Wrongful Accusations Possible

When comparing a single photograph against a database, the study found algorithms were particularly likely to give a false positive for faces of African American females. That could lead to false accusations.
There was a big variation in the quality of algorithms across the study, however. The researchers noted that the less accurate an algorithm was overall, the more likely it was to have significantly different levels of accuracy across different demographics. (Source: nist.gov)

What's Your Opinion?

Are you surprised by the results? Should companies and governments use facial recognition if it is less accurate for some groups of people? Should algorithms have to pass an accuracy test before they can be used by public bodies? ❏

How to stop two Windows Defender annoyances

By Fred Langa

Win10's built-in Windows Defender has matured into a top-ranked anti-malware tool. But several of its default behaviors can be downright irritating.

Here's how to tweak Windows Defender with a few buried settings and a Task Scheduler change.

Plus: Does Adobe Flash Player really need as many updates as it claims?

A pair of improvements for Windows Defender

Windows 10's free, built-in Windows Defender is part of the Win10 Virus & threat protection suite (Microsoft support info).
That, in turn, is part of Win10's truly comprehensive Windows Security suite (MS info), comprising a whole array of useful and effective security tools.
As a whole, Win10's security suite is excellent, and Defender has evolved into a top-ranked antivirus tool, based on independent testing (AV-test.org info). It's fully on a par with third-party offerings.
Still, Defender has a few flaws. Two of the most annoying are ***erratic scans*** and ***too many notifications.***

How to Fix.....................................from page 11

Note — A new (and temporary) Defender flaw: As this article was being finished, Microsoft released a Windows Defender update that caused scan failures on some PCs — reportedly Win7 systems for the most part but also on Win8.1 and Win10. The problematic update is Defender Version 4.18.1908.7. (None of my three physical Windows 10 PCs, nor any of five Win10 VPCs, exhibits the bug.)

To see whether your Windows Defender is working properly, run the "Quick scan" option under Virus & threat protection/Current threats (MS info). If the scan completes normally, you're good to go. On the other hand, if the scan stops after processing only a few dozen files, you have the bug. It's likely Microsoft will have a fix shortly — possibly by the time you read this. Check askwoody.com for updated info. Whether you have the bug or don't, you can still make the adjustments below — they're unaffected. – Fred

How to fix Windows Defender's erratic scanning.

By default, Windows Defender is always on, working in the background, checking each file as it's accessed. But during idle times, Defender is also supposed to perform separate verification scans of at least some files.

If your PC is busy, those verification scans will be delayed — and if delayed long enough to worry Windows, the OS will nag you via a little yellow exclamation mark placed on the Windows Security shield icon (see Figure 1), located down in the notification area. That little warning icon won't go away until you manually trigger a scan or until there's enough idle time for a scan to run on its own.

Figure 1. Windows Security's yellow warning icon (enlarged 200 percent).

Windows' built-in Task Scheduler can help ensure that no future scans are missed. Making a relatively simple change will both enhance your PC's security and prevent that annoying "missed-scan" warning flag from appearing!

Here's how to make the adjustment:

☐   Start typing "schedule tasks" into the Windows search box and select Task Scheduler when it's offered.

☐   In Task Scheduler's left pane, expand Task Scheduler Library/Microsoft/Windows — then scroll down and select the Windows Defender item.

☐   In the top center pane's Name list, double-click Windows Defender Scheduled Scan; a new window labeled "Windows Defender Scheduled Scan Properties (Local Computer)" will open.

☐   In the new window, select the Triggers tab and click New — a "New Trigger" dialog box will appear.

☐   In the New Trigger window, select On a schedule in the Begin the task pull-down menu, then adjust the times/dates to specify when and how often you want the Windows Defender scans to run (for example, daily at 7 a.m.; see Figure 2).
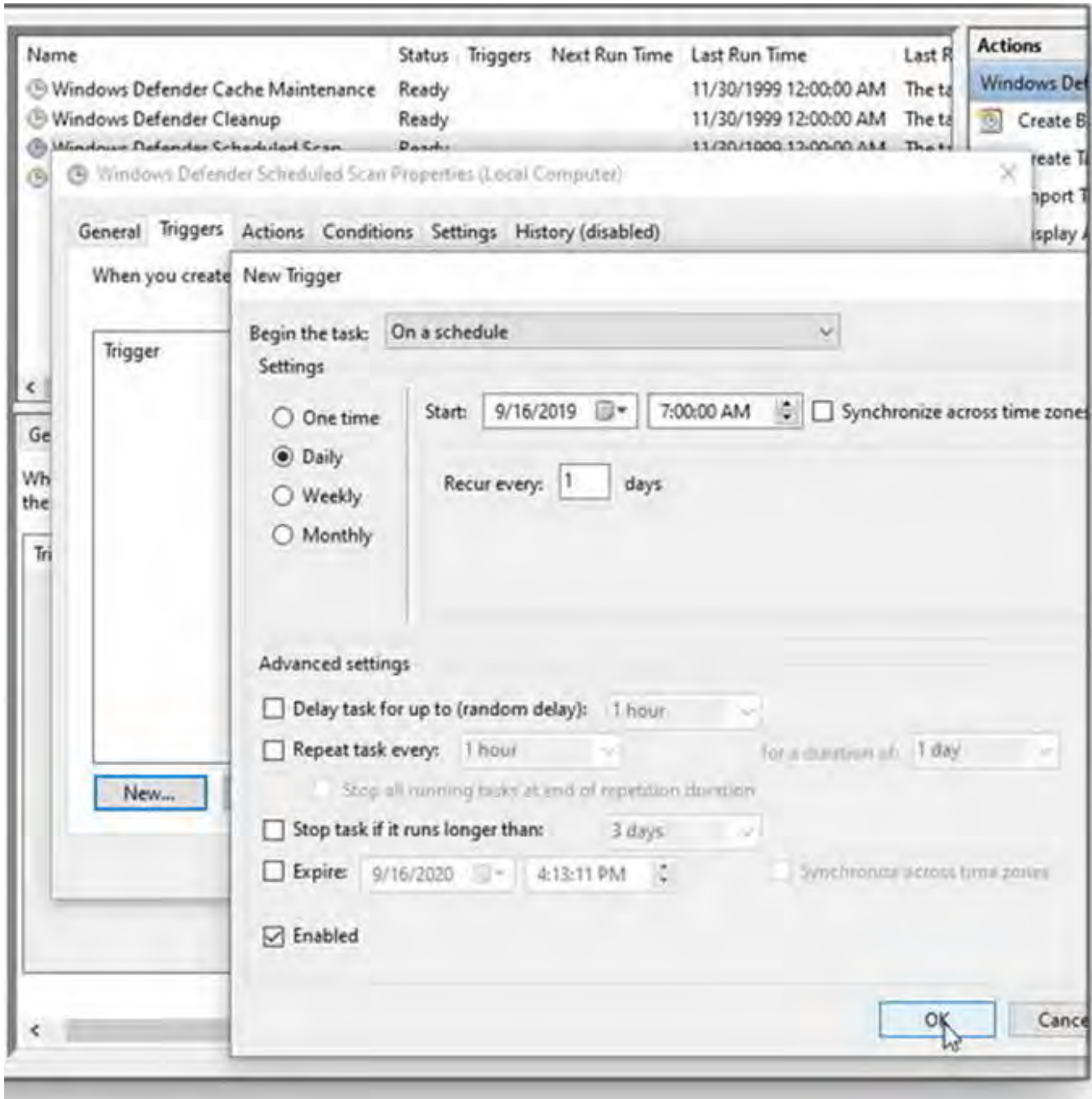
Figure 2. Use Task Scheduler to control the timing and frequency of Windows Defender's scans.

Need further help or refinements? See the Microsoft support page "Schedule a scan in Windows Defender Antivirus."

How to reduce the number of Windows Defender notifications:

☐   Begin typing "security" into the Windows search box and select the Windows Security app when it's offered.

☐   In the Windows Security window, click Virus & threat protection, then click the Manage settings link under Virus & threat protection settings.

☐   Scroll down to Notifications and click the Change notification settings link.
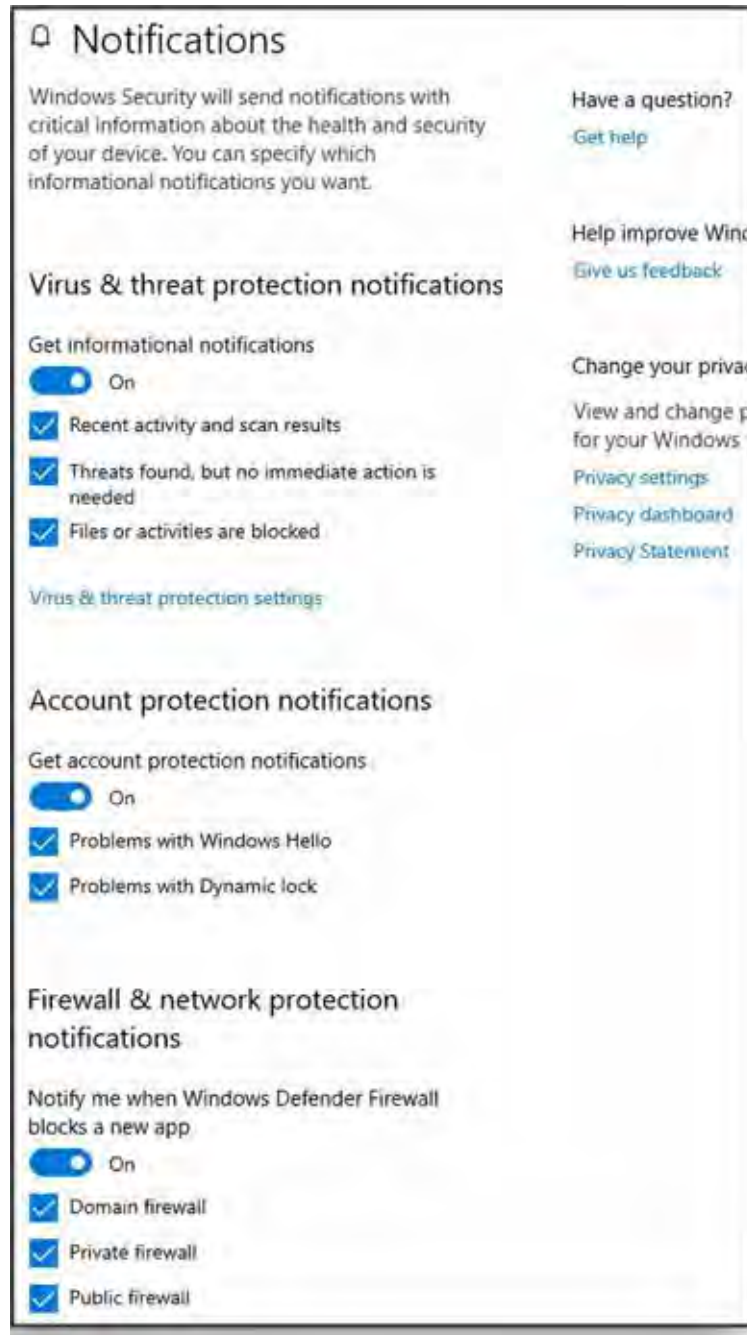☐   Adjust the notification settings as you wish (e.g., as shown in Figure 3).

Figure 3. The Windows Security notification settings are buried a bit, but they're easy to adjust to your preferences.
With Windows Defender reliably performing a daily scan, and with its excessive notifications reined in, you'll have a well-protected PC without needless annoyance! ❑

Texting… Anyone?

By Phil Sorrentino

January 2018 issue, STUGMonitor

Texting is probably more popular than email. Here are some texting statistics I've read from various sources, though I can't really attest to their veracity. From my limited experience, it seems that they are likely accurate. 96% of smartphone users text; Texting is the most widely-used and frequently used app on a smartphone; Over 6 billion texts are sent in the U.S. daily; Texting takes up almost 15% of a cell phone users time; 90% of all text messages are read in under 3 minutes; The average Millennial exchanges an average of 67 texts messages per day; Americans exchange twice as many texts as they do calls; Only 43% of smartphone users use their phone to make calls, but over 70% text (I'm not too sure about that one); It takes the average person 90 minutes to respond to email, but only 90 seconds to respond to a text; Worldwide people will send 8.3 trillion texts this year, that's almost 23 billion per day or almost 16 million per minute. A compelling summary of how smartphone users view texting - they love it. And what's not to love. Texting is a great way of keeping in touch with people in an un-intrusive way. The receiver of a message gets a notification that a message has been received and they can choose to read it or not and answer it if need be. The notification can be a ringer-like sound or as subtle as a vibration of the phone.

Texting and emailing are similar but very different means of communicating. Email tends to be seen as information that can be responded to at a later date. Texts seem to have a sense of urgency attached to them. Maybe it's the way the notification affects us whenever a message arrives. The notification seems to be a lot stronger than just "you've got mail". Watch someone who is really hooked on texting. See how they typically just can't wait to get that phone in their hands so they can answer the text. For some of them, it almost seems like an addiction. For those of us who started with email, long ago, you may remember that instant messaging grew out of email as a way of having the message sent immediately, rather than having it sit waiting for the recipient to collect it. (You may have used AIM, ICQ or MSN Messenger). Texting is today's Instant Messaging. But of course, today you are not sitting at your computer all day, you are carrying your phone with you (all day) so you can be instantly contacted by a text.

Texting is being used for many different purposes. It is being used for personal, family and social purposes among group members; and in business and government organizations for communications between colleagues. Texting originally referred to sending short (less than 160 characters) alphanumeric digital electronic messages using the Short Message Service (SMS), but it has been extended by the Multimedia Message Service (MMS) to include digital images, videos and sound, and now handles messages greater than 160 characters in length. So, texting is the use of these services to send and receive messages and attachments. And it's the texting app on your phone that knows how to use these services to send and receive messages. "Android Messages" is the app that comes on many Android phones. On an Apple device, it is Apple "Messages". But there are many texting apps available for both devices; just check them out at the Google Play Store or the Apple Store.

On the opening screen of your texting app of choice, there will be a way of starting a conversation. On Android Messages, you start by pressing the "+" to start a new conversation. Keep in mind, a text is sent to a phone number, not an email address. So, after your app is opened, you can begin a text, by typing the phone number of your intended recipient using the keypad, or you can find them in your list of contacts. Although there is no 160 character limitation to the size of a text anymore, the size is probably limited by the fact that you are using a

2019 Holiday Party Pictures

Getting the food ready

Before a lot of the food brought in

Now that's more like it

Sandwiches anyone?

Early line entries

Looks just like last year

Line still working - maybe seconds?

Getting ready for the gift swap

Had to explain how it works

We talk and eat at the same time

Looks like everyone's at it

Gene passed around the music, let's sing

Lots of gifts to swap

Lots of fun ---- Check website for 15 more

Texting - Anyone ?....................from page 15

smallish keyboard on the smartphone's screen, where the keys are a lot smaller than the fingers that are poking at them, though I have seen some very fast and deft use of the keyboard with both thumbs moving swiftly across the screen.

Once the recipient's phone number is established, a conversation screen will appear on your screen with the keyboard towards the bottom. (Android Messages also gives you the option to make a phone call from this screen. Why not, it now knows the phone number.) First you create the text by typing the message. Many apps include a feature, sometimes called "predictive text", that attempts to help you with the words and spelling by showing you words it suspects you want. If the word you want shows up, you can touch the word and it will be included and you can go on to the next word. (If you must, special characters and emojis can usually be found somewhere on this screen.)

Once the message is complete, the last thing to do is send it. In this example, the Send command is shown as a paper airplane icon with SMS below it. A short time after your text is sent, if your recipient responds, you will hear your familiar text notification. When you go back into the messaging app you will see the response to your text, as well as your original text. As you continue to interact with the same recipient, the "conversation" will show each of the texts and text responses sequentially. An interlaced series of texts will show up for all the contacts that you have interacted with. You can review this conversation, or any conversation that hasn't been deleted, at any time by choosing the appropriate contact after the app has been opened. You now have a history of all the text interactions with all your contacts that you have texted with. So, now as you have seen, texting is pretty easy to do, and is a great way to keep in touch, in real-time, with some of your favorite contacts. This is probably what has made texting such a popular way to keep in touch. So, maybe some of those surprising statistics are right, after all. ❑

Using the Virtual Desktop (Task View)

By Rosita Herrick, Forum Leader, Sarasota Technology Users Group, Florida

February 2018 issue, STUGMonitor

www.thestug.org
rherrick (at) aol.com

I believe that the Task View option is an ignored productivity feature. Staying productive is often as much about staying organized as anything else, especially while multitasking. And when it comes to productivity on PCs, many people may opt for a desktop setup with multiple monitors. But that's not an option for everyone – particularly if you do most of your work on the go with a laptop.

Thankfully, Windows 10 includes a handy feature that can mimic the experience of spreading your work around multiple monitors without the extra hardware: virtual desktops, or as the shortcut on the task bar displays, Task View. Virtual desktops essentially let you multiply the number of distinct desktops you have at your fingertips on one PC. This can come in handy if you just want to keep work tasks separated from your personal windows. But if separating tasks is your goal, the Task View lets you keep things separate and organized while still having access to everything at a click

How to Use Windows Virtual Desktops

Accessing your virtual desktops is fairly easy, but it's not immediately obvious unless you're looking for it. The most obvious way to get started is through the Task View icon located on your taskbar. You'll find it located to the right of the Cortana search bar; it looks like a rectangle flanked by two other, partial rectangles. Click the Task

View icon and you'll be greeted with a screen that shows all your currently open apps. This is essentially a birds-eye view of your first, primary desktop, which can be quite an asset

On the bottom right-hand corner of the Task View screen, you'll find a "+" icon that says "New Desktop" underneath.

Simply click the button and Windows 10 will surface a bar at the bottom of your screen showing your original, primary desktop and the newly created one.

You can keep tapping or clicking the "New Desktop" button to add as many as you want (based on the capabilities of your PC).

Switching between desktops is as easy as selecting one from the Task view.

View screen. You can also drag and drop specific programs from Task View on one desktop to the others listed on the screen. And when you're done with a desktop, you can close out of it by hovering over it with your mouse and clicking the "X" button within Task View. The benefit of using Task View is that if you close one screen by mistake, the active programs gets transferred to the preceding screen.

Getting around quickly with keyboard shortcuts
Of course, while the steps described above are fine for getting started, you'll want to move around more quickly as you get used to things. Fortunately, there are some keyboard shortcuts associated with virtual desktops that can speed things up.

To access Task View:	Windows key + Tab
Create a new desktop:	Windows key + Ctrl + D
Deleting a desktop:	Windows key + Ctrl + F4 shortcut.
Accessing previous screen:	Windows key + Ctrl + Left Arrow
Accessing next screen:	Window key + Right Arrow

Using the Virtual Desktop...........from page 19

Getting used to the keyboard shortcuts can take some time. However, once you do, you'll find yourself zipping through things at the speed of light.

Task View restricts the user to viewing one desktop at a time. However, the upshot is that it makes it that much easier to quickly switch between tasks without closing one task by mistake. And even if you have ❏

Taking Photos on your iPad and iPhone - the "Camera" and "Photos" Apps

By Jim Cerny, Forum Leader

January 2018 issue, STUGMonitor

www.thestug.org
jimcerny (at) aol.com

Your iPhone and iPad are just great for taking photos. Both devices come with the camera app already installed and it is very easy to use. Touch the app, point your device, make sure it is on the regular "photo" (not video or other setting option) and hit the large white circle to take your photo. After you have taken a photo, it can be found on your device by going to the photos app and looking in the "camera roll" album. That is really all there is to it, but there is even more fun options to play with.

Your device really has TWO cameras, one on each side (front and back) of the device. There is one facing away from you and one facing towards you (to take "selfies"). When using the camera app, touch on the gray circle that has a camera image on it with two circular arrows. This will change the camera to front or back view. Before you take your photo, look for a yellow rectangle which will show you what part of the view is the target of the focus

You can zoom in by touching the screen with two fingers and moving them together. Zooming out (once you have zoomed in) is done by spreading the fingers apart. Wait a moment for the camera to focus before taking your photo.

There are several options for taking photos and new releases of iOS will bring more! Your camera app can also take time-lapse, slo-mo, videos, "square" shaped photos, and pano (panorama) photos. The flash option (a circle with a lightning bolt) can be selected for "on", "off", or "auto". The "HDR" button will take several photos with one click and make one higher quality photo. The HDR option uses more memory per photo. Learn more about this option before you use it.

The "live photo" option (the round button that looks like a target with concentric circles) will take about a 3-second mini-video (with sound) with one touch of the photo button. Your mini-video will consist of several frames from which you can pick one for the best photo. Or, you can just keep the "live photo" as well. Live photos take up more memory on your device. There are several options to play with your live photos too, look for them on Google or YouTube. This is another option that will be well worth your time to learn more about.

In the PHOTOS app you should always review your camera roll album on your device and delete photos you do not want. I think it is best to delete them before you put or "tag" them into an "album". Albums in the photos app help you organize your photos on your device. You could think of an album as a "folder" (a Windows term) but all your photos on your device will always be in the camera roll album. When you put a photo into an album, you are just "tagging" that photo with that album name. Thus, you could have the same photo in multiple albums, but the

photo is only in one place in memory – on the camera roll. If you delete a photo from your camera roll, it can be deleted from ALL albums. But if you delete a photo from an album you will be given a choice to delete the photo OR to simply remove it from the album.

Also, the photos app that comes with your iPhone or iPad comes with a really great selection of options you can play with to have fun with photos. Try changing the color, cropping, contrast, and many more. In addition to all these options (provided free in the "camera" and "photos" app on all iPads and iPhones) you can download any of hundreds of other apps that work with photos.

As with all these fun photo options I recommend that you "Ask Google" or YouTube to learn more about them. If you like to keep things simple, just use the normal "photo" option and keep the HDR and "live photo" options off. But these options can provide you with much photo fun and effects. Why not learn about them? Now give me a nice smile, I want to take your picture.❏

Firewalls
By Dick Maybach, Member, Brookdale Computer User Group, NJ

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

A firewall is a program that monitors traffic on a network and rejects any data that violate its security rules. One way to classify a firewall is by its location: it can be host-based, where it resides on a computer and controls all the data transferred through its data port, or it can be network-based where it resides on a modem or router that connects a local area network (LAN) to the Internet. The latter is sometimes inaccurately called a "hardware firewall," although it is actually software, but running on a router, a modem, or a dedicated processor rather than a general-purpose PC.
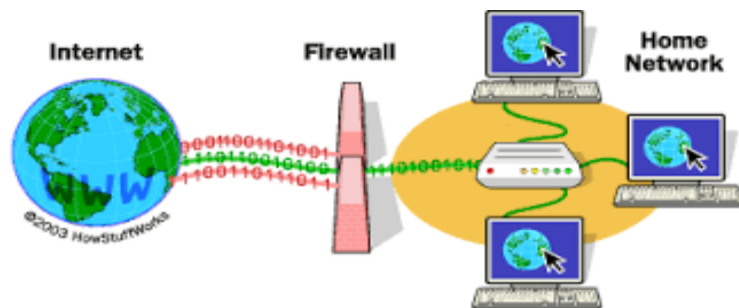

Figure 1. Network-based Firewall.

The primary purpose of a network-based firewall is to isolate your home network from the Internet. Without one, your networked printers, PCs without host-based firewalls, and shared storage devices would be available to the world. A host-based firewall is very similar to a network-based one; the major difference is its location. It isolates the data on your PC, primarily on its disk, from other computers on the network. If you use your laptop to access the Internet through a wireless (Wi-Fi) hotspot, only its firewall protects you. Some firewalls, e.g. that included with Windows, allow increasing the protection when connected to such unprotected networks.

Firewalls...................................from page 21

Figure 2. Host-based Firewall.

There are multiple types of firewalls, each using a different approach to traffic filtering.

- First-generation firewalls were packet filters, comparing basic information, such as the original source and destination of the packet, the port being used, and the protocol, against a list of rules.
- Second-generation firewalls were the so-called stateful firewalls, which added another connection state to the filtering criteria. Based on this information, the technology could determine if the packet was starting the connection, was a part of an existing connection, or wasn't involved at all.
- Third-generation firewalls understand applications as well as some widely-used protocols such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). Based on this information, the firewall can detect attacks trying to circumvent it by misusing a protocol or violating application procedures.

Third-generation firewalls control traffic flow in several ways.

- Service control determines what types of services are accessed.
- Direction control determines in which direction particular service requests are initiated.
- User control determines if a user is allowed access to the service.
- Behavior control determines how particular services are used.

A firewall protects your computer from Internet hacking, where someone gains remote access to it over a network, and against worms, malware that spreads over a network. However, it provides little or no protection against many other threats.

- If you give permission for other computers to connect to yours, e.g. enable remote access.
- Switching off the firewall or adding many exceptions to its rules reduces the protection.
- It is not effective against malware, including viruses, spyware, ransomware, etc. This is most commonly acquired through clicking on email attachments and email links, downloading pirated media, and visiting rouge or infected Websites.
- It does nothing about spam.
- People with physical access to your computer or network are not monitored.
- Data introduced to the computer other than online, e.g. via USB connected devices, CD/DVD etc. are not checked.

- If your laptop acquires malware while connected to a Wi-Fi hotspot, and you later connect it to your home LAN, your other PCs can become compromised since you are behind the firewall.
- Traffic that appears to be legitimate passes freely.
- A firewall protects only information on your home LAN; once you send it to the Internet it's accessible to anybody.
- Only you can prevent phishing, where you are tricked by e-mail, a Website, or a phone call into installing malware, bypassing the firewall, or disclosing sensitive information, such as your bank passwords or credit card details.

If you run a server from home, perhaps to host a Website or exchange files, you need two firewalls, one between the Internet and the network called a Demilitarized Zone (DMZ), and a second one between the DMZ and your home network; see Figure 3. The firewall between the DMZ and the Internet is less secure, because it allows incoming requests to the servers on the DMZ network. Such requests are not allowed through to the home network. Other DMZ architectures may be preferable depending on your requirements. You will need to do some research before implementing one, but fortunately, few home computer users need this complexity.
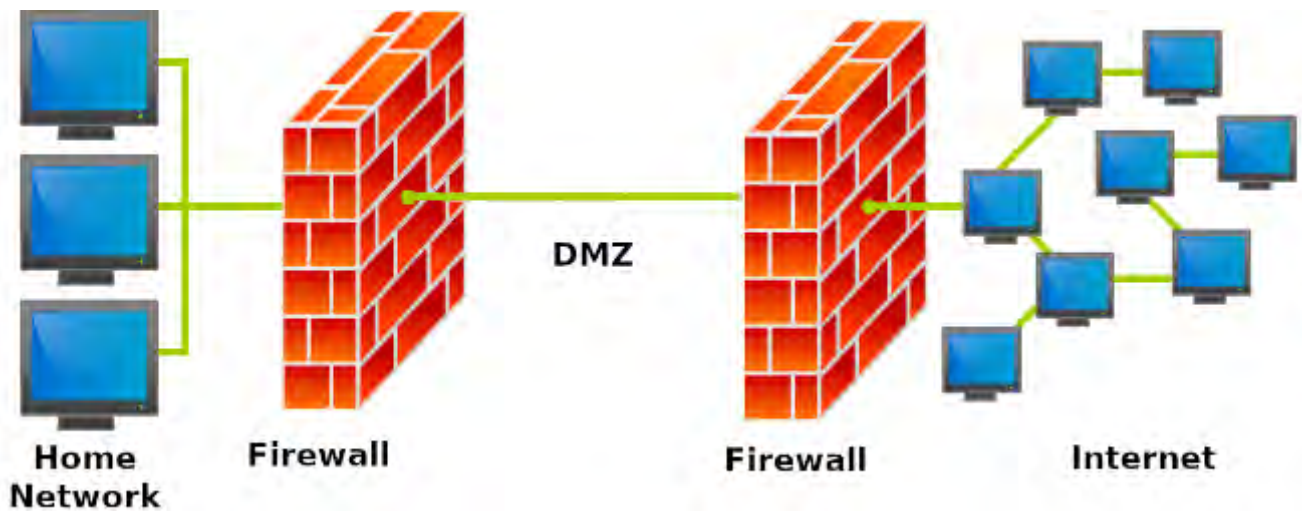

Figure 3. DMZ

Because firewalls are software running on small dedicated processors and are exposed to the Internet, they are subject to hacking, and they are attractive targets. Most home users rely on firewalls included in the cable modems and routers supplied by their Internet Service Providers (ISPs). Unfortunately, ISPs are not diligent in installing patches to correct the security flaws that are frequently uncovered. If the only devices on your home network are PCs with their own host-based firewalls and you haven't enabled file sharing among them, the risk isn't large. However, if you have network-shared storage or other devices without firewalls, you should add your own firewall between your network and the ISP's interface. Many routers include firewalls and these are convenient to use here. Most security experts say that keeping your software up-to-date is the most important security measure, more so even than installing anti-virus software. This applies to any firewalls you install.

Most operating system include a host-based firewall, which is probably adequate for most home users with a network-based firewall between their LAN and the Internet. However, aftermarket software is available from many anti-virus vendors, and you may wish to consider one of these, especially if you have a laptop with sensitive information and use it at public Wi-Fi hot spots. Regardless of how you use it, check your firewall's documentation to be sure it's properly configured for you situation.

You can implement a network-based firewall in three different ways:

Firewalls......................................from page 23

- purchase purpose-built hardware, probably with an integrated router,
- install firewall software on a compact PC such as a Raspberry Pi, and
- install firewall software on a standard PC.

The first is the easiest and by far the most preferable, as it's ready to use right out of the box after minimal configuration. The second requires more work and expertise but can result in a unit that is at least as effective, but few users have the expertise needed to insure the security that this application requires. The third is unlikely to be satisfactory, as PCs have hard disks, monitors, and keyboards which aren't needed here, and you will be tempted to use a surplus one that probably has an old operating system with many known vulnerabilities. You will also have to remove many programs that were needed in its former role as a general-purpose PC but may have security risks. For firewall duty you want simple hardware and software and the latest version of the latter.

A good firewall tutorial is available at http://computer.howstuffworks.com/firewall.htm and a more technical one at http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf . ❑

Six Little Word Problems and their Solutions

By Nancy DeMarte, 1st Vice President, Sarasota Technology User Group, FL

November 2018 issue, STUG Monitor

www.thestug.org
ndemarte (at) verizon.net

1. You print a multi-page Word document and get an unexpected blank page at the end of the document. Because it has a footer, you won't be able to use that sheet for anything except scrap paper.
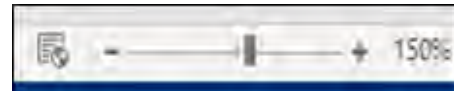
Solution: Before you click Print, press the Show/Hide key on the Home tab > Paragraph group

and scroll or press the Ctrl+End keys to get to the end of the document. You will see one or more   ¶
paragraph icons on the last blank page. Select them and press Delete. Then save the document to avoid the blank page in future printings.
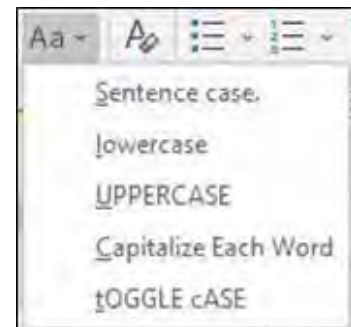
2. You open a document and find you have to squint to see the small type

Solution: Go to the Zoom slider at the bottom right of the screen and click the + sign a few times until the document text is large enough to be comfortable for your eyes. This will not affect the text size when printed.

3. You are just about done typing a Word document and notice that all the text in the last couple of sentences is in upper case. You had pressed the Caps Lock key on the keyboard accidentally.

Solution: First select the text you want to reformat. Then click the Change Case tool (Aa) on the Home tab > Font group. Click the case pattern you want from the list, which in this situation is probably "Sentence case."

4. Sometimes you forget what version of Windows you have on your computer. "Version" includes the operating system (Windows 7, 8.1, or
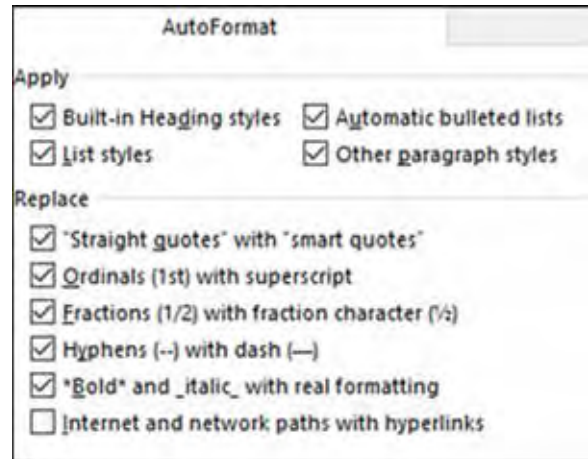
10) and the Windows update version number, such as the recent update, 1803. But you're not sure how to find the answer.

Solution: To find the version of your Windows operating system, type in the Search box at the bottom left of the taskbar the word **winver**. Then click the winver run command to see your computer's details.
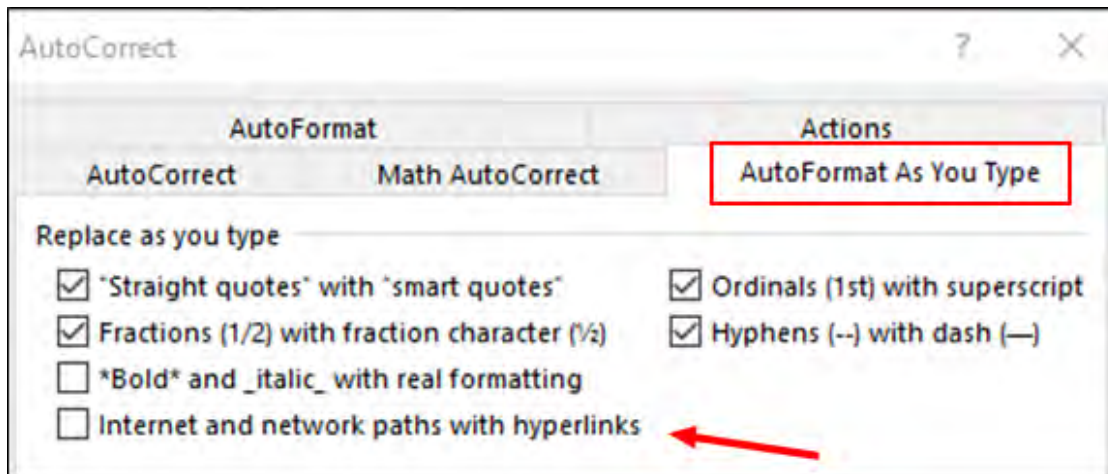

5. When you enter an email or web address in a document, by default Word automatically adds a hyperlink
to the address. You can identify a hyperlink
by its blue text and underline. Many times, you don't
 want the hyperlink included.

Solution: There is a way to change the setting to stop the automatic hyperlink from being added.
Click the File tab (top left of the ribbon), then click
Options (last item on the menu). Click Proofing >
 AutoCorrect options > Autoformat and uncheck the last
item on the Replace list, "Internet and network paths
with hyperlinks," then click OK.

Just to be safe, also click "Auto Format As You Type" and uncheck the same box there, followed by OK

While you are in the Word AutoCorrect area, check to see if you are being bothered by any other automatic action. If so, uncheck it and click OK.

If you change your mind, return to this screen and re-check the boxes.

6. You have typed a long list of items, such as book titles, taking up several pages of a Word document. Each title

Six Little Word.........................from page 25

is on a separate line. You would like to find out how many items there are in the list, but counting them would be tedious.

Solution: Select the entire list using Ctrl+A. Then on the Home tab - Paragraph group, click the numbering tool (top row, second from left) to place a number in front of each item. Then press Ctrl+End to jump to the end of the list, where you can view the last number. If you wish, then press Ctrl+Z or Undo to remove the numbering.❑

Consider the Risks of Helping Friends with PC Problems
By Dick Maybach, Brookdale Computer Users Group, NJ

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

If you are known as a computer enthusiast, your less-experienced friends probably come to you for help when they run into problems. However, you should consider the risks before you agree. While you have a lot of computer experience, most of it is probably limited to your own system, which you are careful to maintain and back up regularly. You also are aware of the risks and avoid suspicious Internet sites, are alert to e-mail scams, and have installed protection against malware. This may not be true of the owner of a PC you are asked to repair.

I once agreed to help a friend who was complaining about his laptop being slow. My first clue that I was in over my head was when I saw the missing keys on the keyboard, but by then I was already committed. I did what I could to clean things up, but the slow processor, full disk, and inadequate RAM remained, and my several hours of work produced little improvement. Another experience was more successful. A PC was thoroughly infected with malware when a teen-age son downloaded pirate music. I cloned the disk, mounted it on another PC, and deleted the problem files. The owner used the restoration partition to put the disk back to its condition when the PC was purchased, after which I loaded their files from the sanitized clone disk. This too took several hours.

Your friends may have unrealistic expectations. If the problem appears to be a full disk or inadequate RAM, the money spent on the parts may not result in a dramatic performance improvement. If you suspect malware and recommend they purchase anti-virus software, it may not fix the problem, and may even slow their PC. You've cost them money without fixing the computer to the degree they expected. And once you've mucked about with their PC, they may suspect that any subsequent troubles are your fault.

Finally, because you are working in an unfamiliar environment, you will probably be spending many hours, even if you aren't successful. Repairing someone else's PC is usually a lose-lose situation. If you fail, you lose a friend, and if you succeed you'll most likely be asked to do it again. The bad habits and poor maintenance that led the initial problem are still present.

If you decide to help, what are some reasonable actions? Your first concern, of course, is to safeguard the owner's information, which means cloning the entire disk (or disks) to an external drive, which can take several hours. Note that this means you copy every byte, not just the complete files. By doing so you may be able to recover deleted and damaged files, directories, and partitions, should that be necessary. If the problem PC is dead, you will of course have to remove its hard disk and install it in a good computer to clone it.

Before you try to diagnose the problem, recognize that you may not be able to trust either the hardware or software in the problem PC. My preference is to use a USB memory stick with a bootable diagnostic operating system, such as PartedMagic, which has tools to check hardware, recover files, and test for malware. (See my

articles in June, July, and August, 2012 on file recovery, in April 2012 and February 2017 on PartedMagic, in May 2015 on the Trinity Rescue Kit, and in June 2015 on the SystemRescueCD, all available at www.bcug.com.) Whichever diagnostic tool you use, become familiar with it on your own PC before trying it on one with which you aren't familiar.

If you save the user's files you should check them for malware before reinstalling them on a repaired or new PC. Take the clone disk home and run a thorough malware check. (Parted Magic, in particular, has the relatively weak ClamAV, which checks only and doesn't repair. If you use Windows, you most likely have far better software on your machine.) Once you have cloned a disk, you can use PartedMagic's tools, or those of a similar system, to recover damaged files. If, as is likely, the problem PC runs Windows, some user data (for example, Internet favorites and e-mail) may be stored in the system area. The locations vary with the version and restoring them in a new system may be difficult. Before spending a lot of time, ask the owner if they really need to recover these.

Although it can be very time-consuming, you can attempt to clean up the file system. This means removing malware, pop-ups, spurious menu bars, and the like. It may also require disabling programs that launch at boot time, and perhaps editing the registry. This is likely to be frustrating as the owner still has the bad habits that caused these problems, meaning the will most likely recur.

Before you agree to anything, try to find out how the problem began. Did they install hardware or software? Did they see a pop-up or get a phone call or message advising them of a problem? Did they visit a new website? Did they delete files or directories by mistake? Did the symptoms appear suddenly of build over time? You are trying to discover whether the problem resulted from hardware failure, software failure, malware, or operator error.

If you have decided to help, this is what I recommend. (Most likely you'll modify these steps to fit your own experience and tools.) Before you begin, be sure the user understands that you are an amateur, and that you can't guarantee success.

- For a casual friend, find out what you can over the phone and recommend a shop.
- If you decide to get more involved, go to the house with a diagnostic USB memory stick and check the hardware and file system. Write down what you find and recommend a shop.
- If this is a very good friend or a close relative, tell them not to use the PC until you can image their PC's disk. (If you don't have a spare USB hard disk they will have to purchase one for the purpose.) Then use your diagnostic memory stick to create an image of the system disk on the external one.
- If the hardware is good, use the restoration partition to return the PC file system to its state at purchase time. (In the unlikely case that the owner has a valid Windows installation disk, you don't need a restoration partition.)
- If the hardware has failed, the owner can decide whether to have the PC repaired or replace it. After this, do what you can to restore the data you have saved, but make it clear that some may be lost.
- Be sure the owner understands that a new PC or a clean install of the operating system means any applications installed after purchase will be lost unless he or she has their original installation disks.
- The last option is to attempt a repair. However, before you jump into this tar pit, be sure the owner understands and accepts the risks. He or she should purchase the parts, with your advice of course. Be sure to make clear that you are amateur in unfamiliar territory and that success is not assured. For example, if the disk has failed because of a faulty power supply, its replacement may be damaged immediately. Who pays?

This is not to say you shouldn't try to help, but it would be prudent to think about your possible approaches as well as the risks before you get the phone call. You don't want to disappoint a friend or cause them to lose money.❏

President's Corner

To Discern the Truth
By Greg Skalka, President, Under the Computer Hood User Group, CA

www.uchug.org
president (at) uchug.org

In the TV game show To Tell the Truth, three contestants all claim to be the same person. Each segment starts with the three lined up next to each other, each claiming to be the described character ("I am John Smith," for example). A panel of four celebrities was tasked with determining which of the three was the real 'John Smith' by asking each contestant (numbered one through three) a set of questions. They knew the authentic 'John Smith' was obliged to tell the truth, while the two imposters may lie. After the period of questioning, the celebrity panelists each record their votes for which contestant they believe is the real 'John Smith', and the real central character is then asked to stand and reveal themselves. The show first aired in 1956, was popular from the 1950's through 1970's, and a revived version has been produced in recent years.

Today we are all unwitting participants in a game played out on the internet to discern the true identities of those we communicate with. Unfortunately, the stakes are higher than some cash divided among the contestants that is proportional to the number of celebrity panelists deceived by the imposters, as in To Tell the Truth. In our game, our confidential personal information, our identities and possibly our finances are at risk.

On the internet, there is a lot of information available, but a lot of it is suspect. Every email, Facebook post, tweet and blog entry could be the absolute truth, totally false or something in between. Even Wikipedia entries could contain biased or even false information, as though they are supposed to be written and reviewed by experts, it is a "crowd-sourced"; encyclopedia. Email is a particularly problematic communications medium for determining the truth of information. The accuracy of statements made in individual emails is obviously subject to the credibility of the sender, and this is usually only judged by the recipient of the email. Unfortunately, it is often difficult to truly know
who the real sender of an email is. For some emails, it is pretty obvious the sender is not the IRS, the Director of the FBI or a Nigerian prince. In other cases, it can be more difficult to verify that the sender is who the email claims. That email from a bank you don't do business with is probably suspect, but what about the emails from banks, utilities, credit cards and other businesses you do expect dealings with?

How do you determine if the email sender is who they claim to be? How do you get them to tell the truth? There are a lot of checks you can make to help discern if an email is authentic and from the source they claim. Look carefully at the sender's email address listed; if the email is from wellsfargo@gmail.com, it is probably not really from Wells Fargo Bank. Even if it looks legitimate, hovering over the address by placing your mouse cursor over the text in the email header may reveal that the actual address is different.

Corporate emails that contain misspellings or grammar issues are probably fake. Emails sent at an unusual time of day for the sender (like the middle of the night) could be suspect. A lot of these are phishing emails, sent by bad people with the hope that you won't notice these inconsistencies and will click on the link included, or open the file attached, actions that will put malware on your device or trick you into entering your real passwords into their fake sites.

I have received my share of phishing emails and think I can spot them in most cases. I know enough to be suspicious and never click on links or open files sent to me, unless I am expecting them or have verified their

authenticity. Last week, however, I was part of a fake email scheme that I had not seen before. I was not the target; the fake emails were sent to others I have corresponded with. Fortunately, these were savvy tech users and it does not appear anyone was taken in by the scam.

I first became aware that something was wrong when I got up on the morning of Monday, April 15 (which was tax day, but I don't think that had any significance). My son sent me a text while I was eating breakfast; he said my UCHUG email address had sent him a strange email at 3 AM and might be hacked. He attached screen shots of the email. The email he had received appeared to come from my president@uchug.org address, and appeared to have two parts, as in an email chain. The first, current part
was a generic message characteristic of phishing emails. It had a zip file attached,
Greg_Skalka_UCHUG.zip. The second part of the email, as if it were a prior part of the email chain, was what I recognized as an actual email that I had sent from a work email to my son over a year ago.

I had my son confirm that he believed the email he received was sent from my UCHUG president email address. I found this to be unusual, as I never send emails from that address. Our group's web hosting and email services are through 1&1 Ionos, and since I am not fond of their email web interface, I have the three uchug.org email address; all are forwarded by the 1&1 email account to my personal email address.

I wondered if someone had actually hacked into my UCHUG president email account but didn't think too much more about it until I started getting more warning emails. Over the course of the morning I received emails from eleven people that had received a similar email from president@uchug.org with the mystery zip file attachment. These included a few of our UCHUG members and officers, a number of APCUG officers and member group officers, and even Bob Gostischa (our March meeting presenter). Most people replied back to me (the UCHUG president email) questioning why I had sent the zip file. A few tried to open the zip but their security software flagged it as infected.
In each case, the emails they received contained the same generic 'Good Morning' message with the same zip file attached. The second part was unique in each email, as were the email subject lines. In most cases that second part was an email that the recipient had received previously, either from me, our editor or another APCUG member.

When I received the first reply at around 7:30 AM, I realized this was likely to be more than just an errant email my son received. I quickly wrote back to the first recipient:
Unfortunately, I did not send you any emails recently. It appears others have been receiving the same email, appearing to come from our president@uchug.org email address. Either that UCHUG email address has been hacked (I'm copying our webmaster so he can look into it) or someone is spoofing that address. In either case, that email is suspect; please don't open its attachment. I don't actually send from the president email address (emails sent to it are forwarded to my personal email), so anything sent from it is not from UCHUG. Sorry - it is sad we live in such a world.
As I received additional replies, I copied that first response and sent it to each, to explain what had happened.

Bob Woods, our webmaster, soon let me know that he could find no evidence that our email account had been hacked, or that these bad emails were being sent from our account. As a precaution, he changed the passwords on my three group email accounts. It appeared that someone was spoofing our UCHUG email address when sending these out. Since there was nothing we could do to stop that, all I could do was continue sending my warning response to all replies I received.

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

Monthly General Meeting Report, December 9, 2019

1. The meeting was called to order by President, Bill Middleton at 3:30 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. This month's general meeting was scheduled to be a briefing by a representative of the State Division of Consumer Services on cyber nastiness currently out to get you via your computer and other schemes and scams threatening Floridians, especially seniors. The President confirmed the speaker on the previous Thursday and left a voicemail with his contact at Consumer Services on the morning of the meeting. No speaker showed up.
4. The ever-ongoing Windows 10 updates were reviewed. No one reported any major problems with Updates, we await the next Feature Update in the spring with trepidation.

5. A lively discussion of security matters followed. The club's recommendations on security software and practices were discussed in depth. Members' experiences were shared. This turned out to be a most interesting meeting – even without a speaker.

6. The meeting was adjourned shortly after 3:30. Discussions continued into the parking lot.

7. Respectfully submitted by Bill Middleton, Secretary. ❑

To Discern the Truth.................from page 29

By early afternoon, the replies to the bad email had stopped. The 'infection' had apparently run its course, with only about a dozen of these impersonating emails sent out, and no one appeared to be the worse for it. Most of the recipients were sufficiently suspicious to not try to open the attachment, and those that did try were protected by their device's security software.

A few days later, Bob Woods sent me an email with a link describing a situation very similar to mine: https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/ This ZDNet article describes how the Emotet malware gang has stolen old email threads (probably getting them from a PC previously infected with their malware), attached an infected document and sent it out to others in the thread. This is possibly what happened with the UCHUG president emails on April 15.

Thus it appears there are bad actors out there, trying to impersonate email users, using old email chains to try to deceive other users into opening their infected attachments. Just like in To Tell the Truth, they are imposters, saying "I am the president of UCHUG," trying to win the game by infecting computers. We all need to be wary and make sure we are certain we know the sender before trusting the message. We all need to ask the equivalent of "Will the real president of UCHUG (or the real email sender) please stand up!"❑

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

Mark Twain

"The only way to keep your health is to eat what you don't want, drink what you don't like, and do what you'd rather not."

"Reader, suppose you were an idiot. And suppose you were a member of Congress. But I repeat myself."

"Get your facts first, then you can distort them as you please."

A slip of the foot you may soon recover, but a slip of the tongue you may never get over.

Beware of the young doctor and the old barber.

All would live long, but none would be old.

Benjamin Franklin

**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

Calendar
of Events

January 16, 2020, 2019   -   SCPCUG Meeting
Merritt Island Library   Auditorium
2:00 PM

January 18, 2020 - Learning Center
Merritt Island Library - Conference Room
12 - 3:30 PM

January 31, 2020   Deadline for Journal Input

February 15, 2020 - Learning Center
Merritt Island Library Conferrence Room
12 - 3:30 PM

February 20, 2020   - CPCUG Meeting
Merritt Island Library   Auditorium
2:00 PM

February 29, 2020 - Deadline for Journal Input

Presentations Schedule
January 16, 2020

The monthly meeting will
be an informal question
and answer session.
Bring your problems
Someone should be able to help

Bring Some Friends or Neighbors

**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.**

**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*

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 _____

Make check payable to: Space Coast PC Users Group
Mail to: SCPCUG , 801 Del Rio Way, #304, Merritt Island, Fl 32953

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, <u>only</u> 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
January 16, 2020

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

To get to Auditorium after entering the front door, go to the seccond door on the left.

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