



PLATEAU PC USERS GROUP, INC GAZETTE



November 2018

Published by the Plateau PC Users Group, Inc. P.O. Box 3787, Crossville TN 38557-3787 www.PPCUGinc.com November 2018

“JOIN US FOR FUN AND LEARNING AT CROSSVILLE’S COMPUTER CLUB”

Volume 24, Issue 11

This Month’s November Meetings

General Meeting
Tuesday, November 13th at 3:00 P.M.
At Christ Lutheran Church FFG

Plateau Photography Club Workshop
Thursday November 15th at 1:00 P.M.
At FFG Library Bldg.
See more information on page #3 regarding
merger of both Workshops.

The November 13th Program at 3:00 P.M.
FFG Christ Lutheran Church

Windows 10 Favorite Features Tips & Tricks

Simple tasks to help you with helpful things you can do in Windows 10 “Tips and Tricks” will be shown in two videos.

A brief rundown will include selected “Tips and Tricks” like:

- Dark Theme.
- Night Light – help with “Blue Light”.
- Print to PDF – built into windows 10.
- Emoji’s in Windows 10 –paste into documents.
- Spatial Sound –tweak built-in speaker, sonic sound.
- Snipping Tool – select areas of screen to copy or print.
- System Restore Point.
- Hidden Start Menu – and other System settings.
- Aero Shake & Snap – hide or open windows Documents.
- Edge Reading View.
- Notification Setting – turning on or off apps.
- Virtual Desktops –get multiple desktops.

Note: We do not publish an issue in December, so this will be the last Newsletter for 2018



We wish you all A Happy Holiday Season and a successful New Year

Inside This Issue	
Club information and Phone numbers	Page 2
Upcoming Events	Page 3
Cool Tips & Site— OneNote Keyboard Shortcuts	Page 3
How to Protect Your Car From a Wireless Fob	Page 4
Add Bookmarks to Your Word Documents	Page 5
Windows Defender Antivirus can run in a sandbox	Page 7
Block calls on your phones and other options	Page 10
Microsoft removes the basic print & scan drivers from Windows 10	Page 11
Organize Your Pictures – Don’t just save them	Page 12
New PPCUG Club Website	Page 13
Software (Apps) Upgrade	Page 14
PPCUG Application for Membership	Page 15
January 2019 Calendar	Page 16

Winter Hours start at **3:00 P.M.** (October through March)
Summer Hours start at 6:00 P.M. (April through September)

Location: Christ Lutheran Church
481 Snead Drive, Fairfield Glade

NOTE: Meeting Dates are now on 2nd Tuesday’s of the month

Join the Club!

Anyone interested to attend the general meeting or any of the SIG meetings as a guest will be charged \$3.00 per person for any or all meetings in that month. Afterwards, you are encouraged to become a member of the Plateau PC Users Group.

Our Club cannot exist without you, the members.

Membership Dues

Our annual dues are now payable July 1st of each year.

Annual dues are \$24 per single person / \$30 per family starting July 1, 2014, with partial years dues as follows:

Due Date	Oct—Dec 2018	Jan-Mar 2019	Apr—Jun 2019	Jul—Sep 2019 Annual Dues
Single:	\$18	\$12	\$6	\$24
Families:	\$22	\$15	\$7	\$30

Student memberships (21 and under) are \$10 annually.

Corporate memberships are \$30 a year for the first two memberships and \$10 a year for each additional membership from the same company.

Contact the PPCUG Treasurer (931) 707-3677

for pro-rated dues of these types of memberships.

BOARD OF DIRECTORS DISCLAIMER

All members of the Plateau PC Users Group are willing to help one another in the area of advice and tutorial instruction over the phone. If you should require more involved services or instruction, we have a few members who are very knowledgeable in several areas. As a responsible consumer, it is up to you to discuss, before retaining a member, any and ALL charges for repair services and time consuming tutorial activities.

It is not the desire of this Board of Directors to set fees for individuals for services rendered, nor the responsibility to intervene between members who enter into a contract among themselves.

The GAZETTE is published using the following: Microsoft Word, Microsoft Publisher, and Microsoft Windows. The Gazette is the monthly newsletter of the Plateau PC Users Group, Inc.

DISCLAIMER: No warranty, express or implied, is made by the PPCUG, the Gazette editorial staff or its contributing editors. This extends to all losses incidental or consequential from the use or non-use of any information in any issue of the Gazette.

All images used in the newsletter, website, blogs, class materials or handouts (“media”) are obtained from a “free use” source, preferably images that have been released as “CCO Public Domain”.

2018-2019 PPCUG, Inc. Board Members



President	Steve Rosenstein	(931) 742-0151
Vice-President/ Compliance	Jim Buxton	(931) 456-6009
Treasurer	John Krueger	(931) 707-3677
Secretary	Cindy West	(931) 484-7306
Past President	Carl Nordeen	(931) 456-5597
Programs	Open	
Membership	John Krueger	(931) 707-3677
Publicity	Mary Anne Nordeen	(931) 456-5597
Gazette Editor	Gordon Botting	(931) 456-2184
APCUG Rep	Steve Rosenstein	(931) 742-0151
Equipment Custodian	Bob Willis	(931) 456-6511
Webmaster	Alan Baker	(931) 788-2201

Directors at Large

Gordon Botting	Richard Del Frate	Barbara Duncan
Bob Willis		

SIG Leader

Plateau Photography Club Workshop	Jim Gries	FGphotography-club@gmail.com (331) 442-9763
--------------------------------------	-----------	--

Up Coming Meeting for January 2019

Note: Change to Winter Hours

The next General Meeting of the
PLATEAU PC USERS GROUP
Will be on **Tuesday, January 8th at 3:00 P.M.**
at **Christ Lutheran Church**
481 Snead Drive FFG
(corner of Snead & Lakeview Drive)

Classes

Please send ideas for new classes to Alan Baker.
(ambaker@citlink.net)

Cool Tips & Sites

Ten OneNote Keyboard Shortcuts.

OneNote is a powerful but underutilized Microsoft Office program, which gives you tremendous flexibility to collect, manage, and share diverse information. The digital notebooks of OneNote can capture text, images, links, tasks, documents, emails, and other key data. Plus, you can share your notebooks with others and synchronize across multiple devices. One way to save time is to learn some of the handy OneNote keyboard shortcuts.

If you are already taking advantage of the power and flexibility of OneNote, try these useful keyboard shortcuts:

- Check spelling: [F7]
- Add current date: [Alt] + [Shift] + D
- Add current time: [Alt] + [Shift] + T
- Add current date and time: [Alt] + [Shift] + F
- Insert a hyperlink: [Ctrl] + K
- Add a new page at the end of the current section: [Ctrl] + N
- Add a new page under current page at same level of indentation: [Ctrl] + [Alt] + N
- Add a new subpage under current page at same level of indentation:
[Ctrl] + [Alt] + [Shift] + N
- Apply, mark, or clear To Do tag: [Ctrl] + 1
- Send selected pages to an email message: [Ctrl] + [Shift] + E

News of the Special Interest Groups

Plateau Photography Club

Beginning in June 2018, the Plateau Photography and Photo Editing Workshop Groups will merge their monthly meetings into one meeting to be held on the third Thursday of each month. As more people take digital pictures, photo editing has become a necessary and essential part of producing the final picture. Since over 95% percent of all pictures taken today are photo edited in some way, it was felt that the two topics should be combined in our meetings.

The meetings will have monthly assignments to take in various categories. Each member will be asked to bring the original picture taken and then explain the photo editing tools used to produce the final picture. There will be discussion covering the picture itself and the tools used and why they were used.

Each meeting will include short presentations on photography practices and/or photo editing techniques. The topics and assignments will be published in advanced to allow enough time for each member to plan and carry out their assignments. Winning pictures will be determined at the end of each meeting. The SIG leader is Jim Gries. at "FGPhotoworkshop@gmail.com"

The Photo Club/SIG website

The Photo Club/SIG website is now up. Access to it is through the PPCUG website, using the "Photo Club" navigation link at the top of each PPCUG page.

***** New PPCUG Website *****

Visit our website at www.PPCUGinc.com. The Learning Center class schedule and Gazette are all available on our web site.

Send your comments and suggestions to the Webmaster, Alan Baker
Webmaster@ppcuginc.com (931) 788-2201

How To Protect Your Car From a Wireless Fob Relay Attack

By Mark Jones Komando.com
TUGNET, 3926 Community Ave, La Crescenta, CA



Your car is always listening. Not for your voice, but for an electronic signal, such as the coded “unlock” signal from your electronic key fob.

If it’s a newer car model, you might not have to press any buttons; just approach your car and the doors will unlock automatically. In some cars, the engine will even turn on.

Wirelessly unlocking your car is convenient, but it can come at a price.

Criminals can easily turn your key fob against you. We’re talking about your key fob’s signal and how easy it is for criminals to intercept. If someone successfully intercepts your key fob’s signal, they can open your car without setting off any alarms.

Also, newer model cars don’t even need a key to turn on the engine. You simply push a button once the vehicle recognizes your key fob, which could be a criminal who stole your signal.

Watch the following video (https://www.youtube.com/watch?time_continue=86&v=8pffcngJJq0) to see how easy it is for a couple criminals to pull this caper off. This footage was recently released by a police department in England.

Always-on key fobs present a serious weakness in your car’s security. As long as your keys are in range, anyone can open the car.

How To Protect Your Car From a Wireless Fob Relay Attack By Mark Jones Komando.com
August 2018 www.tugnet.org the system will think it’s you. That’s why newer car models won’t unlock until the key fob is within a foot.

However, for less than \$100, criminals can get an amplifier that detects key fob signals up to 300 feet away, and then transmits them to your car. In other words, your keys could be in your house, and criminals could walk up to your car and open it. This isn’t just a theory either; it’s actually happening.

Fortunately, there are some simple steps you can take to keep hackers from stealing your signal.

How to outsmart the thief There are a few easy ways to block criminals’ amplified signals. You can buy a signal-blocking pouch that can hold your keys, like the Hack-Blocking Card Pouch sold in the Komando Shop.

(Continued on page 5)

(Continued from page 4)

If you don't want to spend any money, you can stick your key fob into the refrigerator or freezer. The multiple layers of metal will block your key fob's signal. Just check with the fob's manufacturer to make sure freezing your key fob won't damage it.

If you're not keen on freezing your key fob, you can do the same thing with your microwave oven. (Hint: Don't turn it on.) Stick your key fob in there, and criminals won't be able to pick up its signal. Like any seasoned criminal, they'll just move onto an easier target.

Since your key fob's signal is blocked by metal, you can also wrap it up in aluminum foil. While that's the easiest solution, it can also leak the signal if you don't do it right. Plus, you might need to stock up on foil. You could also make a foil-lined box to put your keys in, if you're in a crafting mood.

Add Bookmarks to Your Word Documents

By Nancy DeMarte, 2nd Vice President,
Sarasota Technology Users Group, FL
July 2018 issue, STUG Monitor
www.thestug.org / ndemarte (at) verizon.net

If you have composed a multi-page Word document, especially if it has a table of contents, you can make it easy to go to specific locations within the document by adding bookmarks. A bookmark is used to jump to a place in a document. It is a cousin to a hyperlink, which is most often used to go to a specific place on the Internet.

Let's say you have written a tutorial that has a Table of Contents. By adding a bookmark to each section in the tutorial, the reader can go to any section by clicking its title in the Table of Contents. Anything in a document can be bookmarked: text, a picture, or section, for example. Here are steps for creating a bookmark for section 4 of the tutorial below:

TABLE OF CONTENTS

This tutorial includes a few methods for backing up your PC files:

1. Backing up to a flash drive (page 2-3)
2. Backing up to a CD or DVD (page 4-8)
3. Backing up using Windows 7 Backup and Restore (page 9-10)
- 4. Backing up using Windows 10 File History (page 11)**
5. Creating a System Image & System Repair Disk (page 12)
6. Backing up to OneDrive (page 13)

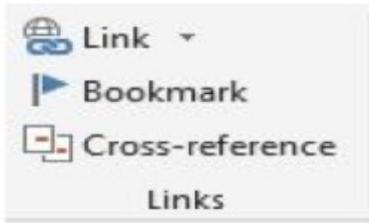
1. Go to and select the title of the chapter where it is located in the document.

4. Backing up using Windows 10 File History

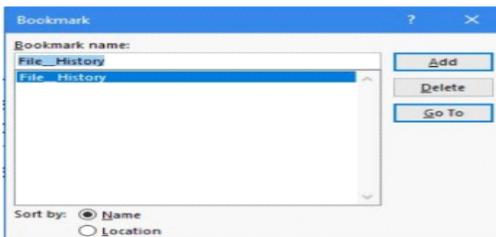
(Continued on page 6)

(Continued from page 5)

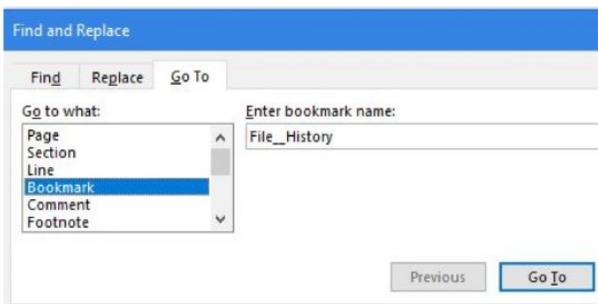
2. On the Insert tab in the Links group, click Bookmark.



3. Under Bookmark name, type a word or short phrase and click Add. (Bookmark names must begin with a letter and must not contain any spaces. They can also include numbers or underscores, as shown.)



4. Test your bookmark by typing Ctrl+G to open the Go To tab in the Find and Replace tool. In this example, we only have one bookmark (File_History). If you have created several bookmarks, choose the one you want. Then click Go To. You will immediately jump to the title of that section.



How to add hyperlinks to get to your bookmarks, rather than use the Find and Replace tool. Below are the steps you will need to create hyperlinks to the bookmarks in your document.

1. Right click the word or image you want to become the link and then left click 'Link'
2. In the 'Link to' box, click 'Place in this Document' (left pane)
3. In the list, select the bookmark you want to link to, and click OK. Now you can use the keyboard combination, Ctrl+click, with each hyperlink to go directly to its bookmark in the document.

Windows Defender Antivirus can now run in a sandbox

October 26, 2018



WINDOWS DEFENDER RESEARCH

in Microsoft 365, Windows, Windows Defender Advanced Threat Protection, Endpoint Security, Threat Protection, Product Updates, Research

Windows Defender Antivirus has hit a new milestone: the built-in antivirus capabilities on Windows can now run within a sandbox. With this new development, Windows Defender Antivirus becomes the first complete antivirus solution to have this capability and continues to lead the industry in raising the bar for security.

Putting Windows Defender Antivirus in a restrictive process execution environment is a direct result of feedback that we received from the security industry and the research community. It was a complex undertaking: we had to carefully study the implications of such an enhancement on performance and functionality. More importantly, we had to identify high-risk areas and make sure that sandboxing did not adversely affect the level of security we have been providing.

While it was a tall order, we knew it was the right investment and the next step in our innovation journey. It is available to Windows Insiders today. We encourage researchers and partners to try and examine this feature and give us feedback, so we can fine-tune performance, functionality, and security before we make it broadly available.

Why sandbox? Why now?

From the beginning, we designed and built Windows Defender Antivirus to be resistant to attacks. In order to inspect the whole system for malicious content and artifacts, it runs with high privileges. This makes it a candidate for attacks.

Security researchers both inside and outside of Microsoft have previously identified ways that an attacker can take advantage of vulnerabilities in Windows Defender Antivirus's content parsers that could enable arbitrary code execution. While we haven't seen attacks in-the-wild actively targeting Windows Defender Antivirus, we take these reports seriously. We immediately fixed potential problems and ramped up our own research and testing to uncover and resolve other possible issues.

At the same time, we continued hardening Windows 10 in general against attacks. Hardware-based isolation, network protection, controlled folder access, exploit protection, and other technologies reduce the attack surface and increase attacker costs. Notably, escalation of privilege from a sandbox is so much more difficult on the latest versions of Windows 10. Furthermore, the integration of Windows Defender Antivirus and other Windows security technologies into Windows Defender ATP's unified endpoint security platform allows signal sharing and orchestration of threat detection and remediation across components.

(Continued on page 8)

(Continued from page 7)

Running Windows Defender Antivirus in a sandbox ensures that in the unlikely event of a compromise, malicious actions are limited to the isolated environment, protecting the rest of the system from harm. This is part of Microsoft's continued investment to stay ahead of attackers through security innovations. Windows Defender Antivirus and the rest of the Windows Defender ATP stack now integrate with other security components of Microsoft 365 to form Microsoft Threat Protection. It's more important than ever to elevate security across the board, so this new enhancement in Windows Defender Antivirus couldn't come at a better time.

Implementing a sandbox for Windows Defender Antivirus

Modern antimalware products are required to inspect many inputs, for example, files on disk, streams of data in memory, and behavioral events in real time. Many of these capabilities require full access to the resources in question. The first major sandboxing effort was related to layering Windows Defender Antivirus's inspection capabilities into the components that absolutely must run with full privileges and the components that can be sandboxed. The goal for the sandboxed components was to ensure that they encompassed the highest risk functionality like scanning untrusted input, expanding containers, and so on. At the same time, we had to minimize the number of interactions between the two layers in order to avoid a substantial performance cost.

The ability to gradually deploy this feature was another important design goal. Because we would be enabling this on a wide range of hardware and software configurations, we aimed to have the ability at runtime to decide if and when the sandboxing is enabled. This means that the entire content scanning logic can work both in -proc and out-of-proc, and it can't make any assumptions about running with high privileges.

Performance is often the main concern raised around sandboxing, especially given that antimalware products are in many critical paths like synchronously inspecting file operations and processing and aggregating or matching large numbers of runtime events. To ensure that performance doesn't degrade, we had to minimize the number of interactions between the sandbox and the privileged process, and at the same time, only perform these interactions in key moments where their cost would not be significant, for example, when IO is being performed.

Windows Defender Antivirus makes an orchestrated effort to avoid unnecessary IO, for example, minimizing the amount of data read for every inspected file is paramount in maintaining good performance, especially on older hardware (rotational disk, remote resources). Thus, it was crucial to maintain a model where the sandbox can request data for inspection as needed, instead of passing the entire content. An important note: passing handles to the sandbox (to avoid the cost of passing the actual content) isn't an option because there are many scenarios, such as real-time inspection, AMSI, etc., where there's no 'sharable' handle that can be used by the sandbox without granting significant privileges, which decreases the security.

Resource usage is also another problem that required significant investments: both the privileged process and the sandbox process needed to have access to signatures and other detection and remediation metadata. To avoid duplication and preserve strong security guarantees, i.e., avoid unsafe ways to share state or introducing significant runtime cost of passing data/content between the processes, we used a model where most protection data is hosted in memory-mapped files that are read-only at runtime. This means protection data can be hosted into multiple processes without any overhead.

Another significant concern around sandboxing is related to the inter-process communication mechanism to avoid potential problems like deadlocks and priority inversions. The communication should not introduce any potential bottlenecks, either by throttling the caller or by limiting the number of concurrent requests that can be processed. Moreover, the sandbox process shouldn't trigger inspection operations by itself. All inspections should happen without triggering additional scans. This requires fully controlling the capabilities of the sandbox and ensuring that no unexpected operations can be triggered. Low-privilege AppContainers are the perfect

(Continued on page 9)

(Continued from page 8)

way to implement strong guarantees because the capabilities-based model will allow fine-grained control on specifying what the sandbox process can do.

Lastly, a significant challenge from the security perspective is related to content remediation or disinfection. Given the sensitive nature of the action (it attempts to restore a binary to the original pre-infection content), we needed to ensure this happens with high privileges in order to mitigate cases in which the content process (sandbox) could be compromised and disinfection could be used to modify the detected binary in unexpected ways.

Once the sandboxing is enabled, customers will see a content process *MsMpEngCP.exe* running alongside with the antimalware service *MsMpEng.exe*.

vmcompute.exe	< 0.01	4588 Hyper-V Host Compute Servi...	Microsoft Corporation	System
vmwp.exe		116 Virtual Machine Worker Proc...	Microsoft Corporation	High
svchost.exe		4596 Host Process for Windows S...	Microsoft Corporation	System
MsMpEng.exe	0.45	4612 Antimalware Service Execut...	Microsoft Corporation	System
MsMpEngCP.exe		12868 Antimalware Service Execut...	Microsoft Corporation	AppContainer
vmms.exe	< 0.01	4660 Virtual Machine Managemen...	Microsoft Corporation	System
svchost.exe		5012 Host Process for Windows S...	Microsoft Corporation	System
svchost.exe		5032 Host Process for Windows S...	Microsoft Corporation	System

The content processes, which run with low privileges, also aggressively leverage all available mitigation policies to reduce the attack surface. They enable and prevent runtime changes for modern exploit mitigation techniques such as Data Execution Prevention (DEP), Address space layout randomization (ASLR), and Control Flow Guard (CFG). They also disable Win32K system calls and all extensibility points, as well as enforce that only signed and trusted code is loaded. More mitigation policies will be introduced in the future, alongside other techniques that aim to reduce even further the risk of compromise, such as multiple sandbox processes with random assignment, more aggressive recycling of sandbox processes without a predictable schedule, runtime analysis of the sandbox behavior, and others.

How to enable sandboxing for Windows Defender Antivirus today

We're in the process of gradually enabling this capability for Windows insiders and continuously analyzing feedback to refine the implementation.

Users can also force the sandboxing implementation to be enabled by setting a machine-wide environment variable (*setx /M MP_FORCE_USE_SANDBOX 1*) and restarting the machine. This is currently supported on Windows 10, version 1703 or later.

Looking ahead: Broader availability and continuous innovation

To implement sandboxing for Windows Defender Antivirus, we took a lot of inputs from the feedback, suggestions, and research from our peers in the industry. From the beginning, we saw this undertaking as the security industry and the research community coming together to elevate security. We now call on researchers to follow through, as we did, and give us feedback on the implementation.

Windows Defender Antivirus is on a path of continuous innovation. Our next-gen antivirus solution, which is powered by artificial intelligence and machine learning and delivered in real-time via the cloud, is affirmed by independent testers, adoption in the enterprise, and customers protected every day from malware campaigns big and small. We're excited to roll out this latest enhancement to the rest of our customers.

(Continued on page 10)

(Continued from page 9)

And we are committed to continue innovating. We're already working on new anti-tampering defenses for Windows Defender Antivirus. This will further harden our antivirus solution against adversaries. You'll hear about these new efforts soon. Windows Defender Antivirus and the rest of the Windows Defender Advanced Threat Protection will continue to advance and keep on leading the industry in raising the bar for security.

Mady Marinescu

Windows Defender Engineering team

with ***Eric Avena***

Content Experience team

Block calls on your phones and other options

By Bart Koslow, Review Editor, Channel Islands PCUG, CA

April 2018 issue, The Outer Edge

www.cipcug.org

bart (at) koslow.net

Whether cell phone or landline phone, we all receive many nuisance calls daily. It is a simple matter to block unwanted calls on most phones once you know how.

Let's begin with your home landline phone. I receive numerous junk calls every day. I use a Panasonic smart home phone system. Like most smart home phones, it permits you to enter your phonebook. You can also set the number of rings before the answering machine kicks in. The LCD on my phone will show me the name of anyone calling who is in my phonebook. Conversely, any name not in my phonebook will also show. The first time I receive a nuisance call I ignore it. My phone will record the name and number of all calls made and keep this information until I erase it. How do I block an unwanted number? I have choices.

My Panasonic will block up to 250 phone numbers. In my case, I use Spectrum (Time Warner) for my landline. You may go to the Spectrum website and block selected calls. You may also check the box that tells Spectrum to use Nomorobo.com. Nomorobo is a large database of nuisance calls. You will hear one ring, and the call will be blocked. For those of you who use other phone providers, you still may use Nomorobo provided the provider has a Simultaneous Ring feature that will ring your phone and Nomorobo at the same time. Furthermore, you may request Nomorobo to add phone numbers to its database by going to its website. Your provider, like mine, may also have a way to block calls on its website.

What about my cell phone? It is even easier to block unwanted calls. If you have an Android phone, just go to Recent Calls, select the phone number and then Details. Under Details you will see a choice to block the call. Depending on the Android version finding the Recent Calls Details varies.

What about you iPhone? Basically, it works the same way if you have IOS 7 or later. Open the phone app. Select the Recents tab at the bottom. Click the 'I' symbol next to the unwanted number, scroll down and tap Block this Caller. Confirm your decision. Microsoft cell phones work in a similar manner. Tap the phone app on the start screen, swipe to history, tap and hold the caller you want to block, and tap block number.

I also have one other option using my Panasonic phone system. You may link two cell phones to the Panasonic

(Continued on page 11)

(Continued from page 10)

phone system. When linked via Bluetooth, the main Panasonic phone unit will show a lighted LED, one for each linked cell phone. When a cell phone call comes in, it will ring on your Panasonic landline system as well as your cell phone. Likewise, you may use the Panasonic system to call out on either of your cell phones. When you finally drop your landline system, the Panasonic Phone system, in my case with five phones around the house, will be a godsend. With unlimited cell phone service becoming extremely cheap, this is an option. Now you can answer or call over your cell phone network from any phone in the house. Even more, the Panasonic system has much better sound.

Hopefully, when you have activated some of the above features, you will have some peace and quiet.

Microsoft removes the basic print and scan drivers from Windows 10.

Windows 10 no longer ships with basic printer and scanner drivers
Now, they are available through Windows Update.

Starting with the October 2018 Update, Windows 10 no longer includes inbox drivers for printers and scanners.

However, it is not the case that the operating system no longer supports these kinds of devices. Instead, the basic print and scan drivers are now available on-demand through Windows Update.

According to the software maker, this decision was made to reduce the footprint of Windows 10 and to free up space on devices.

The company also notes that this change should not impact most users. After installing the Windows 10 October 2018 Update (version 1809), if you have printers previously installed, the device will continue to work using the same driver.

If you connect a new printer after the upgrade, then Windows 10 will automatically download the correct driver from the Windows Update servers.

In the case that your computer does not have an internet connection, then the operating system will install the Mopria-compatible service to send print jobs to the printer without the need to install the required driver.

(Mopria is a wireless printing service designed to connect devices using a universal service, and it works in most wireless printers.)

Of course, you can always install the print or scan drivers manually, instead of relying on Windows Update or the Mopria service.

My Hint: Always go to the printer Manufactures home page and download the latest software for the driver.

It may be better than the Driver that is on the CD included with the printer.

Example: Epson Driver for WF-3530

Organize Your Pictures – Don't just save them

By Phil Sorrentino, Contributing Writer, The Computer Club, Florida
Technical Thoughts, Sarasota Technology Users Group, Florida
<http://scccomputerclub.org> / www.thestug.org
philsorr (at) yahoo.com

How to organize your pictures has been a question since we have had pictures to organize. Before computers, the choices were: put them in an album, or leave them in the packet they came in, or maybe just put them into an old shoe box with all the other pictures. I'm sure many of you have looked through a shoe box of old photos; you might even have inherited a box or two. Many of the pictures in albums or shoe boxes were very precious because there were very few of them. Film was not cheap, and every roll of film had to be sent away for costly processing. With the advent of digital cameras, our picture taking habits have been greatly changed. The job of organizing our pictures has been turned over to the computer, well... sort of. About a year ago, I wrote an article discussing Picture Management. In it, I mentioned that picture management software does not move your pictures; it only lets you view your pictures in a particular way by acting as a lens into your picture collection. The files stay in their place, but the User Interface accesses them in the way that was asked for, like by date, or activity or even by person, and then presents them to you.

As you may know, Google Photos is a picture management App and a cloud picture storage service. If you upload all your pictures to Google Photos, you can get some very interesting organizations of pictures in what they call "albums." Google stores the pictures in whatever way they want and returns them to you in any fashion that you select. Google Photos uses some sophisticated software and facial recognition software to put together albums of a person that you select. It is amazing that they can even pick out side views of a person.

But back to Organizing Your Pictures. One way, that fits into the way that many software Apps work, is to keep "event" folders in chronological order. (Many Apps import your pictures into folders that you can name.) You might then put all the "event" folders for a particular year into a "Year" folder. And to continue that idea, you would put the "Year" folders into the appropriate decade folder. So, in a hierarchical scheme, you would have in your "Pictures" folder, a folder for each decade, and in the decade folder you would have a folder for each year, and in the year folder you would have event folders for the pictures taken at that event.

An organization might look like:

PicturesPS

1980s	would contain 1980 thru 1989
1990s	would contain 1990 thru 1999
2000s	would contain 2000 thru 2009
2010s	would contain 2010 thru 2019
2010	
2011	
2012	
...	And so on to 2018.

I called the Pictures folder "PicturesPS" just to separate it from "Pictures," the folder that comes with the Operating System. "PicturesPS" could be in "Pictures" or in another folder of your choice.

So, once you have the basic chronological folder structure set up, all you must do is create the "event" folders. If you are getting pictures from a camera, there are software Apps that help in organizing the pictures into "event" folders. Microsoft Photo Gallery lets you import pictures from your camera into a folder that you can name.

(Continued on page 13)

(Continued from page 12)

You can set it up to use the current date, like yyyy-mm, and you can add a description, so you have something like “2018-02-Billy’s Birthday” as the event folder and then each of the pictures imported will be named 2018-02-Billy’s Birthday-nnnn” where “nnnn” will start with 0001 for the first picture and increment for each following picture. Photo Gallery is very helpful in organizing your imported pictures and provides a lot of picture editing tools. (After importing a set of pictures, I always seem to need the “red-eye reduction” tool for a few pictures.) Unfortunately, Microsoft does not support Picture Gallery any longer, but if you can get it, it would be a good tool to use to help keep your pictures organized as the size of your picture collection increases.

There are other picture Apps that help in importing your pictures. Faststone Image Viewer provides the ability to import your pictures from a camera but is not as flexible in naming the folder. Faststone also provides basic picture editing tools. XnView, Irfanview, and GIMP are software Apps that provide picture-editing tools and may provide some of the tools you need for keeping your pictures organized. (XnView also allows for importing pictures.)

Importing your pictures from your smartphone may not be as easy as importing them from your camera. But, by one means or another you can probably get the pictures into event folders on the computer. If the method you use allows you to name the picture files, you’re ahead of the game, but my experience has been that the pictures remain named something like “IMGxxxxxxx,” where the xx’s may or may not represent the date the picture was taken. If you do end up with these cryptic names, once you get the pictures into the appropriate event folders you can use an old File Explorer trick to change the picture name of all the pictures in the folder in one operation. Many of you probably remember this from the File Explorer class. With all the pictures in a folder, select the first picture and then Shift-click the last picture. Then, on the first picture do a right-click and select “Rename” in the menu. Next, name the first picture such as “2018-02-15Billy’s Birthday.” All the pictures will be renamed with this name and a number indicating the number of the picture in the selection. Pretty cool.

Now that you have all the pictures in event folders named and the event folders with appropriate names in the year folder, and the year folder in the decade folder, in your Pictures folder, you’re all ready to go out and collect a lot more pictures.

***** New PPCUG Website: *****

You probably have noticed that our website has changed. Alan Baker has been doing the website for over 10 years now and will continue for at least a while. We felt that we needed to modernize by moving the website to an online editing platform versus the current process of local website maintenance, remote hosting and using FTP to upload revised pages and files.

The new online software is easier to use and will allow other trained members to cover for Alan for vacations and the like when needed.

If you have suggestions for changes or corrections to this new website, Please email Alan at “ambaker@citlink.net” .

Our website addresses is still :www.ppcuginc.com



Back to Basics Software (Apps) Upgrades

By Jim Cerny, Instructor, Sarasota Technology User Group, Florida
July 2018 issue, STUGMonitor
www.thestug.org
jimcerny123 (at) aol.com

Software – those programs and apps that you use every day – almost every one of them will require you to upgrade or download a newer version sooner or later. Some apps get updated very frequently, especially the more popular ones. In this article we hope to soothe your fears and give you some helpful tips when doing your upgrades.

You are, hopefully, happily using your device when you get a notice on Windows (lower right corner notification area of your desktop screen) or on your iPad or iPhone (a red circle appears on your “App Store” icon with a number) that updates are waiting for you to download. Almost always you will want to download them – that is, perform the update – soon.

Updates contain “fixes” to the software that the owners of that software would like to make available to you, so that’s a good thing. I also believe that updates also contain new advertising that will display while you are using the app. So, it is a mixed blessing, but you still should install the update anyway.

If you are NOT getting these notices to update, your device may have the option turned on which “auto-updates” your apps for you. Many people may wish to turn on this option.

In Windows 10, you can use the search bar in the bottom left to search for “Windows Update Settings,” when there, select “Advanced Options” and then look to make sure that “Automatic” is selected.

For iOS devices (iPad, iPhone) tap the Settings icon on your home screen, then scroll down to and select “iTunes & App Store”. Scroll down to “AUTOMATIC DOWNLOADS” which then lists the things you may select from – the “Updates” button/slide should be green to have your updates downloaded automatically.

To install updates on your iPad or iPhone, touch the App Store icon and then touch “Updates” at the bottom of the screen. You will see a list (one or more) of the updates that are needed. You can touch each “update” box to do each one individually or you can touch the “update all” box to do them all. A blue circle will fill in gradually to show you the update is being installed.

To install an update in Windows, just click in the notification box that appears and follow the instructions. What I find much easier for me is to use the free utility program/app Glary Utilities. Running Glary Utilities will tell you what needs to be updated on your Windows computer and will allow you to download each update, one at a time. Glary prevents you from searching for the right website and hoping you are downloading the correct update.

Applying updates as they become available is a good idea.

Someday maybe they will have an update to my brain that I can download, wouldn’t that be nice?



January 2019



<u>Sun</u>	<u>Mon</u>	<u>Tue</u>	<u>Wed</u>	<u>Thu</u>	<u>Fri</u>	<u>Sat</u>
		1  <i>Happy</i> <i>New Year!!</i>	2 <u>2:00 P.M.</u> PPCUG Board Mtg.	3	4	5
6	7	8 <u>3:00 P.M.</u> General Mtg. Presentation. Followed By Q&A Session	9	10	11	12
13	14	15	16	17 <u>1:00 P.M.</u> Plateau Photog- raphy Club Workshop Mtg.	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Note: Please see page #15 for the Plateau PC Users Group, Inc. [Application for Membership form.](#)