Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXVI | April 2016 | Issue 4

Meeting Minutes

by Toni Logan, Secretary, P*PCompAS

Next P*PCompAS meeting: Saturday, 2 April 2016
Gene Barlow will give an Acronis webinar.

The 5 March 2016 Membership Meeting was called to order at 9 am by President Cary Quinn. Coffee is free to 1st time guests and a donation for all others. We thank the Starbucks at the Citadel Crossing for our coffee today and at every meeting. There are no guests today.

The minutes of the last meeting were approved as printed in the newsletter.

OFFICER REPORTS

Vice-President Harvey McMinn reported that he has been attempting have someone from Samsung give a presentation at a future meeting. The next meeting in April will feature Gene Barlow.

There was no treasurer's report at this meeting.

Membership Chairwoman Ann Titus reported that all but three of the members from last year have renewed their membership.

Newsletter Editor Greg Lenihan said that Saturday, March 19, 2016 is the deadline for the next newsletter.

Librarian Paul Godfrey needs to update the library from files that are on the website. He also inquired if anyone knows a good catalog program.

APCUG Representative Joe Nuvolini had no report.

OLD BUSINESS

We still need to contact someone in the church as to what they might need so we can give our annual gift to them.

NEW BUSINESS

It was reported that Jim Way's wife, Becky, had passed away. A card from the group will be sent to the family.

The next meeting is on Saturday, April 2, 2016.

AROUND THE ROOM

The audio of the business meeting and Around the Room is on the website.

PROGRAM

The program was a presentation by President Cary Quinn on programs and games to help your memory.

Cary Quinn talks about memory at the March meeting.

DRAWING

Backpack—John Linder
Can of Air—Joe Nuvolini
Android Tablet—Ray Weikart
Monitor—Bob Blackledge ☺

Tip: Windows' powerful, rarely used search tools

Most people search Windows using the Start menu or Windows 8's "start typing to search" Start screen. But for more granular results, try the search box in the upper-right corner of Windows Explorer.

The advanced search tools let you add fancy filters, from date and file type to Boolean operands. This Microsoft page offers a full list of such commands in Windows 7. In Windows 8, you'll find similar functionality in the Search Tools section of the File Explorer's Ribbon UI.

You can create a shortcut to a custom search by simply dragging the magnifying-glass icon in the File Explorer location bar to the desired location. Clicking it will always give you up-to-date results. ☺

In This Issue

Articles

Nuggets from Nuvo
by Joe Nuvolini, P*PCompAS

For the last month or so I have been working on a replacement laptop. It is a refurbished Lenovo ThinkPad T430. I've had a few hard drive issues. Thank goodness I had my Sabrent USB DCS5. I've had it for some time but never have I needed it so badly. I should explain what it is.

The DCS5 is a multi-use, caseless device that allows you to connect 2.5- or 3.5-inch IDE and SATA hard drives, or CD/DVD drives, to your computer via a USB port. I have had to clone drives, wipe them clean, and repartition them during this lengthy process. By the way, just as a matter of interest, I have wiped a number of old drives before disposing them, and while Boot&Nuke does the job, the Acronis Drive Cleaner seems to do it in a lot less time.

Getting back to the DCS5, if you do much drive swapping or wiping, you'll find this item well worth the price. It can be found at the B&H Web site: **http://tinyurl.com/zcyss8e**. The price is $17.24.

BTW, my replacement laptop came with Windows 7 Professional. I did the Windows 10 upgrade so I'm finally in the Windows 10 world. I do like it far better than when I temporarily loaded it on my desktop shortly after its release. Perhaps it's time to upgrade our club laptop. It might be a good program for our May meeting. ☺

Nybbles and Bits
by John Pearce, P*PCompAS

Do you remember Joe Nuvolini's reports on the state of cyber cafes in Italy? The list at cybercafes.com shows quite a few cyber cafes in Australia, however, I noticed just one. It was in the small rain forest town of Kuranda, Queensland. With lots of "free Wi-Fi" signs, it seems like the emphasis has shifted to cellular and Wi-Fi. My wife and I did a land tour in Australia before boarding a cruise ship with ports of call in Australia and New Zealand.

Preparing for the trip, I did some research on cellular service in Australia with the idea of buying a

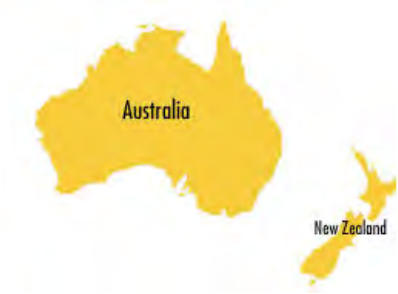
Continued on page 3

Nybbles (Cont. from page 2)

pre-paid phone to use there. This looked like a good option except phone calls and text messages outside Australia were an extra cost. I checked with Sprint, my cellular provider, and found they have a global roaming package at no extra cost. This package provides unlimited text messages (SMS), unlimited data (2G speed), and voice calls to anywhere at twenty cents per minute. In Australia, my phone displayed "Optus" rather than Sprint as the carrier. In New Zealand, it was "Spark NZ." The data speed was not an issue and seemed fast enough for my needs. Maybe it was not limited to 2G speed.

In tourist areas, it seems like there's loads of Wi-Fi access in Australia and New Zealand and some of it is free. The airports in Sydney, Cairnes, and Darwin all had free and unlimited Wi-Fi. My wife and I stayed in three different hotels before boarding the cruise ship. They all had free Wi-Fi although with different limits. One hotel was unlimited access, one was 50 MB per day, and one was free only in the lobby (there was a fee for in-room Wi-Fi access).

Wi-Fi access in restaurants was free and most had a limit either by MB or by minutes connected.



A few restaurants had a small sign with the SSID and password and a few had a sign indicating to ask your server. The server typically produced a small piece of paper with the SSID, password, and the limit. Most restaurants indicated that streaming services were disabled. That restriction eliminates using VoIP protocols like Skype and MagicJack for phone calls.

I overestimated our need to make phone calls on the trip. The concierge at each hotel made phone calls to confirm reservations, arrange transportation, etc., and that eliminated most of the phone calls I expected. We generally used text messages and the GroupMe app to communicate with our family. Text messages moved very quickly. Typical turnaround time was less than a minute although the 17 hour time difference caught me once or twice. For example, Wednesday morning down under is Tuesday afternoon in the US.

There was no cellular service on the cruise ship even though I expected it. The cruise ship literature stated that cell phones should be put in airplane mode to avoid cellular data charges and the Sprint International desk gave me a similar warning. The ship had an Internet Cafe and Wi-Fi on-board for accessing things like the day's events, the ship deck plan, or sales information for future cruises.

On-Board Internet access was an extra cost. I bought a package of minutes just to be sure to have Internet access while at sea. Out on the ocean, interactive Internet access was really slow but was much better when the ship was in port. While at sea, it took about eight minutes to sign in to my Comcast account and display the mailbox contents. Most of the time was probably needed to transfer all the graphic images. By using the e-mail app on my cell phone, I could download new e-mail in about five minutes then read it and write replies while offline.

Overall, I was pleased with the cellular data service and free Wi-Fi while on our trip. Shirley and I were never really out of touch with our family. ☺

It was a brisk Saturday morning on the first day of spring (the Vernal Equinox), but the digerati soon warmed up to good food and conversation. Join us at the Country Buffet on the third Saturday of every month.

The "Internet of Things" or IoT—More Common But Hackable

Published with permission from Ira Wilsker, Golden Triangle PC Club, columnist for The Examiner, Beaumont, TX

WEBSITES:
http://www.cnet.com/news/internet-connected-homes-open-the-door-to-hackers
https://www.cesweb.org
https://www.cta.tech/Blog/Articles/2015/December/VIDEO-The-Wearables-Making-Us-Smarter-More-Fit-an
https://en.wikipedia.org/wiki/Internet_of_Things
https://nest.com
http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home
https://www.shodan.io

A few years ago at the Consumer Electronics Show (CES) in Las Vegas, I was intrigued by the numbers of both prototype and production items that were evolving into what is now known as "the "Internet of Things," or "IoT." For the majority of us, when we think of the Internet, we think of our Internet-connected computers, tablets, and smart phones. What many of us are not well aware of is that the Internet of Things is beginning to be much more common, and the IoT is already around us in a big way.

When I was last at CES, I was amazed at how Internet connections had already made their way into household appliances, and other electronic devices. At CES I saw products being introduced by major appliance manufactures that had connected intelligence built into them.

Among some of the most impressive items that I saw demonstrated were what appeared to be conventional residential kitchen refrigerators that had what appeared to be a flat screen tablet on the front of the door, as well as other types of sensors and readers built into the appliance. The tablet on the front door could be connected to the Internet via Wi-Fi and used to order groceries from participating supermarkets, display recipes, and create shopping lists. A small bar code reader was installed on the door that could read the UPC codes on products, adding those items to a digital shopping list that could be remotely printed, or sent directly to the chosen supermarket. The tablet on the refrigerator door would also display digital coupons and other promotions, enabling the owner to instantly add the promoted item to the grocery list.

This Internet connected refrigerator, as well as IoT connected washers, dryers, dishwashers, air conditioners, stoves, ovens, microwaves, and other major appliances also incorporated a "service connection" which monitored the physical operating condition of the appliances. These appliances utilizing their Internet connection, typically Wi-Fi, would report their operating condition, suggest repairs and maintenance, provide or order a list of replacement parts, display do-it-yourself repair instructions, or contact a repair service if necessary. Most of these devices would actually send an e-mail or text message to the appliance owner alerting him of the issues.

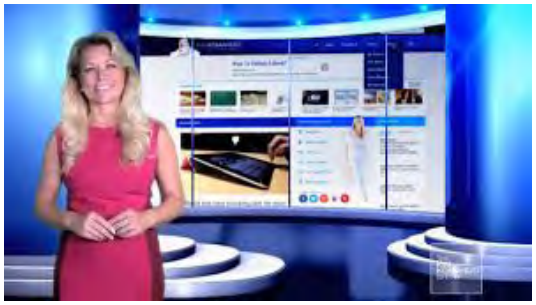
Many auto manufacturers currently offer "OnStar," "BlueLink," or other types of cellular or Internet connected monitoring systems that can report on maintenance issues, service reminders, and other issues, as well as providing a method of emergency communications. My wife's car periodically sends her an e-mail listing the mechanical condition of each of the major components on her car.

We are seeing much more of our homes being controlled or secured by the IoT under the general topic of "Building and home automation." Most modern home security systems can be remotely accessed and controlled by cell phone; security cameras can display their images on remote devices anywhere. Lamps can be remotely controlled to turn on or off by remote command. Even our utility usage and thermostats can be accessed remotely. The very popular Nest thermostat, along with an increasing number of competitors, offers Internet connected control of household temperatures, as well as smoke detectors and remote cameras. My new "smart TV" is connected to my home data network, which allows me to use my smart phone as a fully functional remote to not just control the TV, but to also search through

Continued on page 5

7 Tech Myths You Believe That You Shouldn't

by Kim Komando (tip from 1/29/16)



Technology used to move forward like a freight train (literally at one point), but now it's more like a 300 mph bullet train. You just have to blink and you'll miss the latest smartphone, processor upgrade, new type of connector or any dozens of other developments that never seem to stop.

With technology arriving this quickly, information about how to use it correctly can come and go just as fast. Yesterday's standard operating procedure is tomorrow's mistake. And what used to be good advice for avoiding danger might not be relevant anymore.

Today, we're going to tackle seven persistent tech myths that started out good, but that you really shouldn't believe anymore. These cover the range from battery charging to data disposal to privacy and general tech buying. How many of these did you already know?

You Shouldn't Charge Your Gadget Overnight

Many people are afraid to charge their phone or tablet overnight because they think it might overcharge and destroy the battery. I also field this question from people worried about leaving laptops plugged in 24/7.

Fortunately, you can stop worrying. Modern electronics automatically stop before the battery overcharges. As long as you don't put your smartphone under your pillow, or stab a battery with a kitchen knife, you're OK. Learn more about battery safety and how to make your batteries last longer.

Continued on page 7

Internet of Things (Cont. from page 4)

dozens of streaming media services to watch countless movies, TV shows, videos, and other content, all connected by my home Wi-Fi network.

A review of local industry, health care facilities, public utilities, transportation systems, and other commercial enterprises are rapidly becoming more involved with the IoT. Look at your water, gas, and electric meters; many are already Internet connected in order to speed automate "meter reading," saving time and money. In the medical field, health monitoring and diagnostic equipment is becoming more connected to the Internet. According to Wikipedia, "These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers or advanced hearing aids. ... Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. ... Doctors can monitor the health of their patients on their smart phones after the patient gets discharged from the hospital."

While much of this current IoT technology is infringing on what used to be in the realm of science fiction, there is also a dark side to the IoT. Already, hackers are breaking into Internet-connected devices other than the traditional computers and data networks in order to illicitly control these IoT devices, alter or steal data and personal information, or shut them down on demand. In terms of connected medical devices, there have been some serious concerns expressed about complying with HIPAA and other privacy and security rules and regulations.

It has been well documented that some common household smart devices, most notably smart TVs, have actually spied on their owners. This was reported about two years ago in Forbes magazine by Joseph Steinberg, in his expose' "These Devices May Be Spying On You (Even In Your Own Home)." On January 27, 2014, this article in Forbes said, "Televisions may track what you watch. Some LG televisions were found to spy on not only what channels were being watched, but even transmitted back to LG the names of files on USB drives connected to the television. Hackers have also demonstrated that they can hack some models of Samsung TVs and use them as vehicles to capture data from networks

Continued on page 6

Internet of Things (Cont. from page 5)

to which they are attached, and even watch whatever the cameras built in to the televisions see." Internet-connected coffee makers, which can be remotely programmed to make morning coffee may disclose to hackers when you may be waking up, and even what time you might be returning home; valuable information for residential burglars. The smart refrigerator may be selling your shopping information to third parties. In an unexpected and unusual case, Joseph Steinberg reported that a smart refrigerator was used to send out spam emails, " ... (P)otential vulnerabilities have been reported in smart kitchen devices for quite some time, and less than a month ago a smart refrigerator was found to have been used by hackers in a malicious e-mail attack. You read that correctly – hackers successfully used a refrigerator to send out malicious e-mails." Also in that Forbes article, companies providing DVR, satellite, and cable service have been alleged to have sold information of shows and other content watched in the household in order for advertisers to better target their advertising. It is also widely known that many Internet service providers compile lists of websites visited; since many people get their TV and Internet from the same provider, these companies could combine that information, which Forbes warns, "a single party may know a lot more about you then you might think."

Another popular target for hackers and other miscreants is common household video capture equipment, such as a webcam or a home security camera; remote baby monitors are similarly targeted. Forbes disclosed that malware on a computer can remotely turn on and off the Internet-connected cameras. In one notable case referenced in the Forbes article was how a Miss Teen USA was allegedly blackmailed by a hacker who controlled her laptop's integral webcam, " ... and photographed her naked when she thought the camera was not on." The images of home security cameras, often transmitted unencrypted over the Internet, can be captured by burglars, informing them that not just is the home currently unoccupied, but also the location of the potentially incriminating cameras!

Information about specific items connected to the Internet is readily available, and even searchable as easily as any other Internet data. The Shanghai-based website Shodan (shodan.io) describes itself as, "Shodan is the world's first search engine for Internet-connected devices."

On the front page of Shodan is a self aggrandizing statement that says, "Explore the Internet of Things. Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them," followed by, "See the Big Picture - Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!" Just as an experiment, I registered on Shodan with a disposable email address, and did a quick search of my neighborhood; I found nine potentially vulnerable IoT connected devices within a small radius of my house. I also found that some local service stations monitor their gasoline inventory in real time, transmitting their data in real time over an unencrypted Internet connection. For example, when searched, one particular major refiner branded station reported, "IN-TANK INVENTORY Regular 7263 (gallons), Temperature 51.74 degrees" as well as other inventory information. This was one of 45 "Automated Tank Gauges" reported by Shodan in this area. This gasoline tank information was just a very small snippet of the millions of such Internet connected devices that most of us have no idea even exists.

In a December 28, 2015 article published by Cnet, "Internet-connected homes open the door to hackers," with the subtitle, "Baby monitors, thermostats, kitchen gadgets and other "smart" devices add convenience to our daily lives. What are manufacturers doing to make sure they don't make life easier for criminals too?" The author, Laura Hautala, explained the vulnerabilities of our household IoT. In the opening of the article, employees of a Sunnyvale, California cybersecurity company, Fortinet, used the Shodan search engine to find a video stream in Saudi Arabia, 8100 miles away. Using the too common factory default username and password of "admin", they were able to view the streaming video. According to Fortinet engineer, Aamir Lakhani, the Shodan search engine can display, "... a huge trove of Internet-connected devices, from baby monitors to cars, cameras and even traffic lights." Sadly, many of these devices still use factory default usernames and passwords, and transmit their data over unencrypted Internet links. The Cnet article goes on to state, " Billions of sensors will soon be built into appliances, security systems, health monitors, door locks, cars and city streets to help manage energy use, control traffic, monitor air quality, and even warn physicians when a patient is about to have a stroke."

The Cnet article stated that a well respected

Continued on page 7

7 Tech Myths (Cont. from page 5)

Don't Use Third-Party Chargers

There is a difference between knockoff chargers and third-party chargers. A third-party charger is an Apple- or Android-compatible charger from a reputable company like Belkin or Monoprice. Third-party chargers are OK to buy. Just know that, in general, they won't charge your gadget as quickly or reliably as a maker's official charger.

Knockoff chargers usually don't have a brand name, or they say they're from Apple, Samsung, HTC, etc., but have a ridiculously low price. Knockoffs are often responsible for the horror stories you hear about gadgets bursting into flames or electrocuting users. Avoid them at all costs.

Your safest choice is to buy your charger directly from the gadget manufacturer. You should also know the signs of a shady gadget charger.

You Have to Let Your Battery Drain to Zero Before Charging

Nickel-Cadmium batteries, which used to be a staple of home electronics, had a "memory effect." That meant if you didn't drain them fully before each charging, they'd eventually stop holding as much electricity.

The Lithium-ion batteries that have replaced them in modern gadgets don't have that problem. In fact, Li-ion batteries last longest when you keep them between 40% and 80% charged. Also, if you let Li-ion batteries discharge completely for too long, they can be permanently damaged or become dangerous as we explain here.

But Li-ions do have one challenge. The batteries have a built-in sensor that tells your gadget how much electricity is left in the battery. Over time, that stops matching up with the battery's actual charge. To reset it, you have to charge the Li-ion battery to full, let it run down to the point where your gadget gives you a serious battery warning and then charge it back up to full again. However, this only needs to be done every three months or so.

For some gadgets, you might not need to do it at all. Apple used to recommend this process but now says it is no longer needed. Check your gadget's manual to see if it has any specific directions.

Always Shut Down Your Computer at Night

This myth goes all the way back to the early days of computers. Back then, computer parts, especially hard drives, wore out much faster than they do today. So, the idea was that to make your computer last longer, you should always shut it down at night. Some people still cling to that concept, and there is a little grain of truth in it.

However, modern computers have more robust parts, which means you can let them run with little to no problem. Whether you shut down your computer nightly now just comes down to personal preference. If you want your computer to do things like back up, update or other intensive tasks, you can schedule them at night while

Continued on page 8

Internet of Things (Cont. from page 6)

market forecaster, Gartner, predicted that in 2016 there will be 6.4 billion Internet connected devices in use. Many new IoT devices will be displayed and demonstrated at this year's CES in Las Vegas. Among some of the risks of an insecure IoT could be a variety of malicious vandalism, as well as outright identity theft, terrorism, and crimes of opportunity. Tanuj Mohan, co-founder of Enlighted, gave one such potential example of vandalism. He was quoted in Cnet as saying, "That connected coffee maker in the office -- it wouldn't be much of a stretch for a hacker to put it into a continuous loop and brew coffee throughout the weekend, flooding the office. ... When computers hold the reins, criminals can grab control in unexpected ways." At present, there is no coordination or uniform standard for IoT security, and many manufacturers of IoT devices do not incorporate adequate default security into their devices, making the aggregate vulnerability of the devices potentially catastrophic. Mohan warned that manufacturers are not paying attention to the potential security vulnerabilities of many of their products. "They're not yet aware of how everything they build can be exploited. Safety last."

We, as users of IoT products need to take some personal responsibility for the use of our connected products. We should never use any default usernames and passwords such as the "admin" used to give total access to video link mentioned above, but instead use difficult to guess passwords. Since many of the devices offer some form of encryption as an optional setting, it would be wise for all users to engage that option, and set a complex pass phrase for a decryption key.

The Cnet article closes with a very prophetic statement. "Baby monitors, thermostats, kitchen gadgets and other "smart" devices add convenience to our daily lives. What are manufacturers doing to make sure they don't make life easier for criminals too?" ☺

7 Tech Myths (Cont. from page 7)

you are not using your system.

If you're concerned about saving energy, turn it off. Or you can use one of your computer's many power-saving modes, which are faster for getting it going again in the morning.

You Need to Defragment Your Hard Drive

This is a myth that used to be true, but no longer is. Given the way conventional magnetic hard drives read and write data, over time bits of data that should be next to each other get jumbled. So, to pull up a file, the drive would have to travel to 15 different places instead of 1 or 2, which slows down your system.

It used to be that you'd occasionally need to manually run a utility to defrag your system. Now, that function is built into Windows and other major operating systems, and it's run it automatically as needed. There's no need for you to do a thing.

In fact, defragmenting can even cause a problem if you're using a solid-state hard drive. Not only do SSDs not have fragmentation problems, the memory cells are only good for a certain number of reads and writes. Running a defragmenting program just wears out your drive faster.

You Can Completely Wipe Data

Hopefully, you know that when you delete a file from your computer it isn't gone for good. It's still hanging around on your hard drive waiting for another file to overwrite it. Until that happens, you can recover it.

That's a problem if you're selling or giving away a computer; you never know what information a computer-savvy person can pull from the system. You need to make sure the data is gone for good, but how?

In the olden days of magnetic media with early hard drives and floppy disks, waving a magnet over the drive or disk would do the job. However, modern hard drives are much more resistant to magnetism, so that won't work.

The generally accepted way to wipe your information is with a program that overwrites your hard drive with random data several times. That way, there isn't anything to recover. Learn the detailed steps to wipe your computer or mobile gadget here.

That's fine for conventional drives, but because of the way solid-state drives work, both in computers and mobile gadgets, you can never be sure you've gotten everything. Mobile gadgets do include a reset feature, and many SSDs come with their own wiping software. However, something might get missed.

In most cases, no one is going to go looking for what's been left behind, or get anything too important. However, if you're really worried, you can keep your gadgets at home and use them for other projects. You can also remove your hard drive from the computer before giving it away and store it, turn it into an external drive, destroy it, or make art with it.

Interesting fact: Since 2007, the federal government mandates that for hard drives and other media that have contained classified material, the only option is to completely wipe and then destroy them.

Private Browsing is Totally Private

Every Web browser has a private mode. When private browsing mode is on, the browser won't record where you go and it wipes most of the information someone using the computer could use to piece together your online travels.

In Microsoft Edge, Internet Explorer, Firefox and Safari, you enter private browsing mode using the keyboard shortcut CTRL + SHIFT + P (CTRL + OPTION + P on Mac). In Chrome, you use CTRL + SHIFT + N (OPTION + SHIFT + N on Macs). Click here to learn more about private browsing and how you know you're in private browsing mode.

What you might not know is that private browsing isn't foolproof. It doesn't hide your browsing from your Internet service provider, the sites you visit or any law enforcement that happens to be watching. Ditto if there's a logger on the computer or the router is set to record sites visited. Like most things in tech, private only means that it's harder to find.

Bonus: More is Always Better

This is a general myth that tech manufacturers love because it boosts sales. However, it isn't always true, and sometimes more can even hurt you.

You might be deciding between a laptop with a 256 gigabyte solid-state hard drive and a 1 terabyte conventional hard drive. A 1TB drive is four times larger, but an SSD is much faster and more reliable. Plus, most people rarely even fill up a 256GB hard drive.

Similarly, you shouldn't automatically buy the camera with more megapixels or the smartphone with the highest-resolution screen. In a camera, image quality is as much about the size of the image sensor as the number of megapixels.

With smartphone screens, after a certain point you can't tell the difference in resolution (and most high-end and mid-range smartphones are past that point). However, a higher-resolution screen burns battery life faster. ☺

Back to Basics: Getting Devices to Work Together

By Jim Cerny, Columnist, Sarasota TUG, FL, www.thestug.org, jimcerny123 (at) gmail.com

Every year I hear that the wonders of technology are going to make our lives easier and easier. Do they mean less confusing? I don't think so! We have smart phones, tablets, touchscreens, laptops, desktops, printers, high-tech television, all kinds of internet services, cable boxes, upgrades, new software, and computers in our cars almost ready to take the wheel. The problem is getting all these devices, all made by many different manufacturers, to work together! They said it would be easy to get phone calls in my car, get free internet TV programs on my TV, get my e-mail on my phone and tablet, and watch any video on any device. (Well, maybe watching a football game on my car computer would not be such a good idea while I am driving). Thus we can spend many hours trying to get one device to communicate with another.

Maybe some day you can just turn on your new device for the first time and it will somehow know all your other devices and quickly set them up to work together. But will I see it in my lifetime? I don't think so. Well, what do we do now? What steps can you take to make things easier? I hope the following tips may help.

1. Read the instructions for your device. If it did not come with an instruction book, look it up on the internet.
2. Find all the buttons, indicator lights, and all other hardware things you can press, click, switch, or plug things into. This is not as easy as it seems since manufacturers hide buttons and make them the same color as everything else. (Why do they do that? Are they ashamed that they have an "on" button??)
3. Follow the instructions for setting up your device. If you have to enter some kind of ID (login, or account number) and a password, WRITE IT DOWN and don't lose it. It is always immensely more difficult to help someone who has lost their ID or password.
4. Use the internet to find out more and ask/enter very specific questions. Use Google or YouTube. Enter something like: "How do I read my Gmail on my iPhone?", or: "How do I get my HP Office Jet Pro 8600 to work with my Toshiba Laptop with Windows 7?" Be as specific as you can with the make, software version, model number, etc.
5. Try to get a book at the library to help you. Ask the librarian for help.
6. Ask the manufacturer or the place where you purchased your device. Call them first and ask if they can help (some may never want to talk to you again after they have your money). Take the approach that you spent a good deal of money to buy the device and if you cannot use it as it was advertised you will return it for a refund.
7. Find someone who has the same device as you and ask them how they use it.
8. If all the above fails, you may have to take your device(s) in to a professional – a computer help/repair place or have one of their techs come to your location. Try to explain the problem on the phone first and ask how much such a fix would cost. If they do come to your home, make sure you TEST ALL your devices involved before you let them leave. They may fix one problem on one device, but that does not mean it will now work with other devices.

If you experience some success, go celebrate with a dinner out. Then, hopefully, you will remember the nice dinner instead of the frustration you experienced getting things to work. Well, technology advances on and, so long as there is money to be made by coming out with new devices or upgrades, you can be sure such progress will continue. Maybe some things are passing us by, but let's try to keep moving ahead anyway even if we are a bit slower than others. ☺

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 2 Apr beginning at 9 am (see directions below)
Next Breakfast Meeting: 16 Apr @ 8 am, Country Buffet, 801 N. Academy Blvd.
Newsletter Deadline: 23 Apr.

Check out our Web page at: http://ppcompas.apcug.org