Bits of Bytes

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

Volume XXXV | August 2015 | Issue 8

Next P*PCompAS meeting: Saturday, 1 August 2015
The presentation will be on Genealogy.

The Prez Sez

by Cary Quinn, President, P*PCompAS

As we look forward to another fascinating presentation on Genealogy this month, we also enter the season of new releases in anticipation of the return to school season. I hope your summer is going well. ☺

Meeting Minutes

by Toni Logan, Secretary, P*PCompAS

The 4 July 2015 meeting was called to order by the President Cary Quinn at a little after 9:00 am. He wished everybody a "Happy 4th of July." He reminded us that coffee is free for first-time guests and a donation for all others. The coffee is still provided by Laura at Starbucks.

The minutes were approved as printed in the newsletter.

OFFICER REPORTS

Programs are set for August and October, otherwise the Vice-President had nothing else to report.

The Treasurer's report was presented by member John Pearce in lieu of Dennis Conroy who was not in attendance. We have a total of $7072.90 in the treasury.

Editor Greg Lenihan reported that the deadline for the next newsletter is on Saturday, July 18, 2015 which is the same day as the breakfast.

Neither the Library committee, Hospitality committee, nor the Board of Directors had anything to report.

APCUG Rep Joe Nuvolini reported that the new website will be featuring user groups and ours will be there sometime in the future. He will let us know when.

Media representative Ilene Steinkruger reported that she had e-mailed information for Focal Press to the members.

OLD BUSINESS: None

NEW BUSINESS: None

AROUND THE ROOM

The audio for Around the Room is on the website.

PROGRAM

Four of our members gave short presentations at the July meeting; Ann Titus, Ilene Steinkruger, Cary Quinn and Paul Godfrey.

Ann Titus

Ilene Steinkruger

Cary Quinn

Paul Godfrey

There was no drawing at this meeting. The next meeting is on Saturday, August 1, 2015. ☺

In This Issue

Articles

P*PCompAS

Nybbles and Bits
by John Pearce, P*PCompAS

Is one piece of hardware adequate to run both Windows 10 and Android? That is the question I have worked to answer over the last month or so. The idea is to run both operating systems on one piece of hardware. It saves a few dollars buying hardware and it is one less thing to carry around.

There are a number of PCs that convert to a tablet form factor by detaching the keyboard. Some PCs, like the Microsoft Surface products, consider a keyboard to be optional. Most of the screens for the convertible devices are in the 12" to 14" range while the largest tablets are generally in the 10" range.

Screen resolutions for tablets range from 1024 by 600 up to 2560 by 1600 for the high-end Samsung tablets. The Microsoft Surface Pro 3 screen resolution is 2160 by 1440. The Surface 3 resolution is 1920 by 1280. Any of these are adequate to display HD video. A touch screen is typically standard in the convertible PC products but not always. For my purposes, a touch screen is mandatory. Running Android with only a mouse is like running Windows 8/8.1 with only a mouse - not very pleasant.

Running the Android OS and apps on PC hardware requires an emulator. There are several different emulators available with different levels of features and capabilities. Some are free and others require purchasing a license. Emulators are generally sensitive to the version of Android. For example, one emulator might run Android 4.4 KitKat OS while another might run Android 5.0 Lollipop OS.

The emulators also have their own operating system and hardware requirements. For example, one emulator may require Windows Pro 7 with 2 MB RAM available and screen resolution of at least 1280 by 768. Some emulators run as a Windows application and one emulator is built to use the Oracle Virtual Box, which is the same package I use to run Windows 10. The emulators appear to require either Windows 7 or 8/8.1. Official availability on Windows 10 may have to wait until Win 10 is formally released.

I have decided to try the AMIDuOS emulator. It is a paid product ($9.99) with a 30-day free trial. It is a product of American Megatrends who may be best known for their PC BIOS chips. The current production product is Android Jellybean (4.1 - 4.3). The current beta product is Android Lollipop (5.0). It has a number of favorable reviews, is preloaded with the Amazon Appstore, and is reported to be easily connected with the Google Play Store. ☺

Nuggets from Nuvo

*by Joe Nuvolini, P*PCompAS*

I had another Acronis True Image save recently. As I have probably mentioned earlier, I am moving from my old Windows XP desktop computer to my Windows 7 HP computer. I had HP photo printing software on my XP machine and wanted to install it on my HP. I use it almost exclusively when I am printing photos on my HP Photosmart printer. I had the CD, but it was a home made one and it wouldn't install on the Windows 7 machine. I did a Google search looking for an answer to my problem. On a forum I found a solution. Apparently, the program is almost self-contained. The recommended solution was to copy the program directory from the old XP computer to the HP computer. I opened the Acronis image I had of the XP C drive using Windows Explorer and copied the HP photo printing directory to the HP and created a shortcut to the executable file. However, when I ran the program, it reported a missing DLL. I again loaded the XP image in Explorer and copied the missing DLL from the Windows System 32 directory on the XP computer to the same directory on the HP. That being done, the program ran fine. The missing DLL is why I said earlier that the program was almost self-contained. It's amazing how much time and energy Acronis True Image has saved me over the years.

If you have had your laptop for a number of years, you might want to check the status of your battery. Recently I was having trouble getting my laptop to reboot after some Windows updates. It seemed that I had to let the computer sit idle for a short time before I rebooted it. If not, it would try to reboot and then shut down. At some point I decided to check the battery. It turned out that even with the AC power plugged in it would only charge to 44%. I ordered a new battery from Amazon for about $20 and it charged right up to 100%. That's the good news. The bad news is that it didn't fully resolve my reboot problem. However, it's still a good idea to check your laptop battery from time to time.

Since ComputorEdge ceased publishing in March, I am unable to get media credentials for next January's CES. I started to register as a non-media attendee and found that for the first time they are charging a $100 registration fee for next year's show. I decided I will pass on it. Thus comes to an end my string of having attended either COMDEX or CES every year since 1989. I guess all good things must come to an end! ☺

Android Factoid: If you're asking what's with all the sugar, according to Google "Since these devices make our lives so sweet, each Android version is named after a dessert."

Version 1.5 = **Cupcake**
Version 1.6 = **Donut**
Versions 2.0 through 2.1 = **Eclair**
Versions 2.2 through 2.2.3 = **Froyo**
Versions 2.3 through 2.3.7= **Gingerbread**
Versions 3.0 through 3.2.6= **Honeycomb**
Versions 4.0 through 4.0.4 = **Ice Cream Sandwich**
Versions 4.1 through 4.3.1 = **Jelly Bean**
Versions 4.4 through 4.4.4 (and 4.4W through 4.4W.2) = **KitKat**
Versions 5.0 through 5.1.1= **Lollipop**

The Country Buffet booked our normal room to a group of local Marines (Oorah), but offered us a discount on our breakfast by moving us to another area. It worked out fine. The food was just as good and so was the camaraderie.

Tips to Protect your Privacy Online

By Tim Hoffman, P*PCompAS

1. Use your own computer if you can. It's generally safer to access the Internet from your own computer than from other computers. If you need to use a computer other than your own, you won't know if it contains viruses or spyware. If you do use another computer, be sure to delete all of your "Temporary Internet Files" and clear all of your "History" after you log off your account or put the browser into "Incognito Mode" (Chrome) before using the network.

2. Use a smart and strong password for EVERY ACCOUNT. Having one password for all accounts is the worst thing to do. If the password and e-mail address that you use for one account gets in the hands of the wrong person, they can start trying it on other sites and services. Make sure you use different passwords on different sites. Consider a password manager as soon as you have more than 4 sites to log into. Last Pass was recently broken into and others are also free and likely to have vulnerabilities – but this is better than trying to remember 35 or 40 USER ID/Password combinations. Also, USE PASSPHRASES and keep the resulting passwords long. Passphrase composition can be made up from personal experiences.

3. Set up two-factor authentication to provide an extra layer of security where possible. When you sign into your account, it requires you to enter another code, which you can only get via text or a voice call. This way no one can get into your account unless they have that piece too.

4. Beef up your computer's security. Install antivirus and antispyware software from companies you trust. Password-protect your wireless router, and use flash drives cautiously. Make sure the computer you are using has the latest security patches, and make sure that you access the Internet only on a secure web page using encryption. The website address of a secure website connection starts with "https" instead of just "http" and has a key or closed padlock in the status bar. NOTE: For help with securing your home network, contact Tim Hoffman Associates.

5. Be aware. Even if a web page starts with "https" and contains a key or closed padlock, it's still possible that it may not be secure. Some phishers make spoofed websites that appear to have padlocks. To double-check, click on the padlock icon on the status bar to see the security certificate for the site. Following the "Certificate Information" in the pop-up window, you should see the name matching the site you think you're on. If the name differs, you are probably on a spoofed site.

6. Don't respond to e-mails requesting personal information. Legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as e-mail. If you have reason to believe that the one who e-mailed you actually does need personal information from you, pick up the phone and call the company yourself for verification. Even though a web address in an e-mail may look legitimate, fraudsters can mask the true destination. Rather than merely clicking on a link provided in an e-mail, type the web address into your browser yourself or use a bookmark you previously created.

7. Don't reveal too much on social networks. Don't post anything online you wouldn't want to see on a billboard. Guard account numbers, user names, and passwords with special care. Adopt tight privacy controls to manage who can see your profile or photos, how people can search for you, and who can make comments, and to block unwanted access.

8. Spot the signs of a scam. Watch for deals that sound too good to be true, phony job ads, notices that you have won a lottery, or requests to help a distant stranger transfer funds. Other clues include urgent messages ("Your account will be closed!"), misspellings, and grammatical errors.

9. Avoid cookies. Cookies download themselves from sites you visit. At times they might seem to be helpful as they can remember what you looked at last, but they can also track you online and allow someone to create a profile of you without you knowing it. You can set your browser to reject cookies or at least delete them often using the advanced preferences.

Continued on page 5

Windows 10 for PCs and Tablets Available on July 29

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

WEBSITES:
http://blogs.windows.com/bloggingwindows/2015/02/10/how-cortana-comes-to-life-in-windows-10/
http://blogs.windows.com/bloggingwindows/2015/06/01/hello-world-windows-10-available-on-july-29/
https://www.microsoft.com/en-us/windows/windows-10-faq
http://www.cnet.com/news/minecraft-windows-10-edition-coming-july-29/
https://www.microsoft.com/en-us/windows/features
https://www.microsoft.com/en-us/windows/windows-10-upgrade
http://www.techradar.com/us/news/software/operating-systems/windows-10-release-date-price-news-and-features-1029245
http://blogs.windows.com/bloggingwindows/2015/07/02/windows-10-preparing-to-upgrade-one-billion-devices/
http://www.extremetech.com/computing/191279-why-is-it-called-windows-10-not-windows-9
http://www.pcworld.com/article/2690724/why-windows-10-isnt-named-9-windows-95-legacy-code.html

Earlier this year, I wrote about some of the potential features that were being considered to be included in the upcoming release of Windows 10. The release version of Windows 10 is now complete, with Microsoft already producing packaged software for the retail channels, while PC manufacturers are already producing machines with Windows 10 factory installed, to go on sale on July 29. Some of the big box stores and online sellers are already taking "presale" orders for Windows 10 software ($119 retail), and computers to be delivered or otherwise made available on the official release date. In the coming few weeks, watch for the inevitable media blitz promoting Windows 10.

For almost all users of Windows 7 and Windows 8 (8.1), Microsoft will be offering a free upgrade to Windows 10; contrary to some independent blog posts, the free copy downloaded and installed under this limited time offer will remain free, without any future annual fees. At a recent computer club meeting I was asked about the strange new icon that suddenly appeared in the system tray on Windows computers; this small icon looks like a window frame, with four quadrants, turned left at about a 45 degree angle.

Continued on page 6

Privacy Online (Continued from page 4)

10. Avoid bogus file downloads. Be wary of any website that requires you to download software to view a page, unless it's something familiar like a Flash plug-in or Acrobat Reader. The file may contain a virus, a Trojan horse, or some auto-dialer that calls pay-per-minute numbers via your modem and racks up huge charges.

11. Use extra caution with wireless connections such as those found in coffee shops. Wireless networks may not provide as much security as wired Internet connections. In fact, many "hotspots" - wireless networks in public areas like airports, hotels and restaurants - reduce their security so it's easier for individuals to access and use these wireless networks. Unless you use a security token, you may decide that accessing your stuff online through a wireless connection isn't worth the security risk.

12. Make sure to use a firewall. A firewall is a must today – it acts to bounce signals away that are not associated with any requests to the Internet you have made. It really is like a bouncer at a club that keeps out unwanted elements (except it is for your computer). It checks every ID at the door and won't let anything in or out until you give the thumbs up. So a hacker has a harder time of gaining access to personal information on your hard drive, and a Trojan horse or keystroke logger can't steal your passwords and transmit them over the Internet.

13. Back up your data files at least weekly (daily if you're running a business). Even if you fall victim to a virus or hacker attack, you'll escape with only minor damage. Being able to get back to known good is critical. If you don't know what GOOD looks like – you can't return there.

14. The best tip of all is to use common sense! Situational awareness is very important. If something doesn't feel right, it probably isn't. If something seems to be too good to be true – IT IS ! ☺

Windows 10 (Cont. from page 5)

Moving the cursor over the icon, it simply says "Get Windows 10." Clicking on the icon opens a small window, "How to get Windows 10 for free!" While some of those at the computer club meeting were suspicious about the offer, it is indeed legitimate, and is being made by Microsoft. The new Windows 10 release mentioned is a complete version, free for life (rather than the $119 for a boxed retail version), that will be available for download on or after July 29. I would not try downloading Windows 10 in the first few days, as it is a very large 3 GB download, and Microsoft and its partner servers will be hammered by the users trying to get the new software. In some published reports, Microsoft is predicting that up to a billion copies of Windows 10 will be downloaded and installed starting on July 29. Some Internet pundits are also warning of a possible Internet slowdown starting in late July as the digital "pipes" become "clogged" (overloaded) when many millions of users try to download a 3-GB file.

The release version of Windows 10 has incorporated many of the suggestions made by Windows 8 users, who missed some of the familiarity and ease of use that was available in Windows 7, but not incorporated in Windows 8. Among the most requested features that has been included in Windows 10, and that was missing in Windows 8, is the traditional "Start" menu, which will help Windows 7 users become immediately familiar with Windows 10. Windows 10 has been designed to boot quickly, and be more secure than previous versions of Windows. According to Microsoft, Windows 10 will incorporate its own antimalware security software; Microsoft stated that Windows 10 will include, "... Windows Defender for free anti-malware protection, and being the only platform with a commitment to deliver free ongoing security updates for the supported lifetime of the device."

Windows 10 was also designed to run on almost all computers capable of running Windows 7 and 8, without substantial hardware upgrades. According to an official Microsoft blog posting, "We designed Windows 10 to run our broadest device family ever, including Windows PCs, Windows tablets, Windows phones, Windows for the Internet of Things, Microsoft Surface Hub, Xbox One and Microsoft HoloLens—all working together to empower you to do great things." Microsoft is obviously creating a seamless way for users to move

between many different devices, using the same, familiar operating system.

Windows 10 will include the much discussed Cortana, which Microsoft describes as, "The world's first truly personal digital assistant helps you get things done. Cortana learns your preferences to provide relevant recommendations, fast access to information, and important reminders. Interaction is natural and easy via talking or typing. And the Cortana experience works not just on your PC, but can notify and help you on your smartphone too." The somewhat archaic Internet Explorer browser, which grew out of the old Mosaic browser, will be replaced by a leaner and more efficient new browser which Microsoft is calling "Edge." Edge will be integrated with Cortana, allowing users to more efficiently interact with the Internet with voice, keyboard, or other forms of input.

As is now common on smart devices running Google's Android, and Apple's iOS, the new Windows 10 will have its own "app store" where both paid and free apps (what we "used" to call software) can be downloaded directly from a Windows store. Also at the Windows store will be a huge collection of games, TV shows, music files, movies, and other content to download. Android and iOS users may notice a similarity with the Google Play Store or iTunes, and the new Microsoft store, as they will all function in a similar manner.

One of the most popular digital games of all time, Minecraft, will be available for Windows 10 on the official release date of July 29. Since Microsoft purchased Mojang, the Swedish authors of Minecraft for a reported $2.5 billion last year, and released builds of Minecraft for other Microsoft platforms and devices, it was inevitable that Microsoft would have a build of Minecraft optimized for Windows 10. Officially, the Windows 10 version of Minecraft released in a few weeks will be a "beta" or prerelease version of the popular game. Users of the current PC versions

Continued on page 7

Windows 10 (Cont. from page 6)

of Minecraft will get a free upgrade to the Window 10 build, and others may purchase a full version of Minecraft for $10, including free future updates.

One of the features touted by Microsoft with the new Windows 10 release is the ability to integrate Xbox gaming with the PC and tablets running Windows 10. Xbox Live and a new Xbox app will be incorporated in the new release, giving users access to the well established and popular Xbox Live gaming network.

Microsoft has announced a new Office suite, Office 2016, which has been specifically written "from the ground up" to run efficiently on any devices running Windows 10. The Office 2016 components Outlook (e-mail program) and OneNote (digital note taking) will be included with Windows 10, while individual apps for Word, Excel, and PowerPoint will be available, presumably for sale, from the Windows Store. Microsoft said that all Office 2016 components will seamlessly run across a variety of devices. Using touch screen devices, Office components such as Excel will be touch enabled, and can be created or updated without using a mouse or a keyboard.

An improved security feature intended to restrict unauthorized access to a device running Windows 10 is "Windows Hello," which will incorporate biometrics to verify authorized users. Windows Hello can use facial recognition, finger print scanning, and iris scanning to instantly verify users, instead of using the more traditional (and vulnerable) password method. Once a user is authenticated by the Windows Hello service, the user will be greeted by name, and with a graphical smile on the screen; while some beta users initially thought that this friendly response was cute, others found that it eventually became somewhat irritating.

Microsoft is also including a series of integral apps with Windows 10 to perform some of the users' most common tasks. These apps will handle photos, videos, maps, e-mail, calendar, music, contacts, and other functions that smart phone users are already somewhat familiar with. Since Windows 10 will also be incorporating Microsoft's cloud storage service, OneDrive, content will also be securely stored in the cloud as well as on the device. Since Windows 10 is explicitly designed to run on multiple platforms, the appearance and functionality of these apps will be the same on all devices. Content created on any device will be securely stored in the cloud, and readily available on any other compatible device. Microsoft says, "You can start something on one device and continue it on another since your content is stored on and synched through OneDrive."

If you have the Windows 10 icon in your system tray, open it and sign up to reserve a free copy of Windows 10 when it becomes available. Even if you do not have that Windows icon that recently appeared, you may still be eligible for a free upgrade. Once the mad rush of those who will clog the Internet by being among the first few million to download and install Windows 10 is over, and the Internet traffic jam subsides, I will be downloading and installing Windows 10 on my computers. Since "Murphy's Laws" are endemic on computers of all types, I strongly recommend making both an image backup and a critical data backup of your current setup before installing Windows 10. If for some reason you don't like Windows 10 after installing it, the image backup copy can be used to restore your earlier operating system. Backing up critical data files should always be done "just in case."

While I have been generally satisfied with my Windows 7 installation, and found Windows 8 to be not quite as user friendly, I look forward to the upcoming release of Windows 10 and the free upgrade offer.

Just to satisfy the curiosity of my readers who may have noticed the jump from Windows 8 to Windows 10, whatever happened to Windows 9? The truth is that there was no Windows 9, and Microsoft purposely skipped the moniker "9". Some Microsoft pundits have alleged that the "9" was skipped to avoid confusion with those users still running the long obsolescent "legacy" Windows 95 and 98. Since "9" was skipped, "10" was the logical next version number; "Windows X" was considered, but there already was a Mac version "X." Microsoft has been inconsistent with version names anyway, having used dates (95, 98, 2000), names (Vista, Bob, Millennium), and simple numbers (3.1, 7, 8, 8.1). There has been no consistent naming or numbering convention, so the Microsoft leadership decided that "10" would simply describe a totally new operating system. Whatever it is called, I suggest that eligible users download and install the free upgrade, and try it. The new release combines the best features of Windows 7 and 8 (without 8's foibles), and adds a lot of new features and functionality, as well as seamless integration across multiple devices.

As the old cereal commercial said, "Try it ... you'll like it." ☺

12 Security Terms You Need to Know

by Kim Komando (tip from 2/14/13)

Let's start with some security terms that keep popping up in the news.

Drive-by download - When malware takes advantage of security flaws in your programs to download to your computer without your permission. All you have to do is visit a website that hosts the malware and your computer is infected.

Zero-day exploit - A serious security flaw that exists in a piece of software before it's released. If hackers can find and use it before the developer releases a patch, they can do serious damage.

Backdoor - A secret entrance to your computer that lets someone bypass your security. You won't even know they're inside! Backdoors come from program flaws or are intentionally built into software by the developer.

Drive-bys, zero days and backdoors are all dangers of flawed or out-of-date software. Three of the worst offenders are Java, Flash, and your browser. So be sure to keep these programs updated or disabled.

Security software can protect you from these dangers, too.

Now, on to the malware:

Virus - A piece of software that can copy itself and spread, just like a biological virus. This is the most recognizable term because it's been around the longest.

It can infect different parts of a single computer or grow to infect multiple systems. In the past, viruses would destroy your data or cause other chaos. These days, they're a bit more refined.

Worms - An advanced type of virus that replicates and spreads with little or no action on your part.

You can get a worm as a Trojan (more on that in a bit) or from a drive-by download. If you're on the same network as a computer with a worm, it can infect your machine with little effort.

While worms are serious if left unchecked, any up-to-date anti-virus software can handle them.

Botnet - A collection of computers that has been infected with a specialized virus, usually a worm. The hacker that created the worm can control the infected computers, sometimes called "zombies."

A botnet can send spam, launch attacks on websites, funnel stolen money around the world, or anything else a hacker wants. In fact, most of the spam you get is from botnets.

The best way to stop a botnet is for everyone to have security software installed and up to date. Most people with zombie computers don't use security software and have no clue their computer is compromised.

Trojan - The most popular kind of attack online. Also called a Trojan horse, which makes sense if you know Greek mythology.

Like the original Trojan horse, a computer Trojan looks like something good - a cool video or photo - but when you bring it inside your computer, it turns out to be malware. Trojans are usually spread through email attachments and often act as a backdoor for hackers. Once installed, a Trojan can steal information or install other, more dangerous, malware.

Rootkit - A more advanced version of a Trojan. "Root" in computer lingo almost always means increased or unlimited control. If a rootkit is installed on your computer, a hacker can do just about anything they want to your machine.

Even worse, a rootkit can hide itself from your operating system and security software, making it hard to detect and remove. Security software is better at dealing with rootkits than it used to be, but it still isn't a pleasant experience.

Like a Trojan, the best way to stop a rootkit is to avoid installing it in the first place. Follow the same precautions you would take to avoid a Trojan. And keep your programs and anti-virus software updated, as new rootkits appear regularly.

Ransomware - Spooks you into surrendering your hard-earned cash. Sometimes called "Scareware," this nasty malware can take many forms.

One common version is a fake anti-virus program that claims you have multiple viruses and need to pay for a full version of the program to get rid of them. Having real security software installed is your best defense.

Nastier versions take over your computer and accuse you of inappropriate activity such as viewing child porn or illegal fire-sharing. Some versions just claim to have encrypted all your files. Either way, the ransomware demands payment to give your system back.

Paying up won't do anything but encourage the hackers. You'll need a heavy-duty anti-virus program to get rid of ransomware. AVG's bootable anti-virus disk is a good solution. Make sure you read the

Continued on page 9

Tip: How to Find the Wi-Fi Password of your Current Network

by Amit Agarwal, Digital Inspiration, http://www.labnol.org/software/find-wi-fi-network-password/28949/

Your computer is connected to a Wi-Fi network but you do not remember the password that you had earlier used to connect to this particular Wi-Fi network. Maybe you forgot the password or maybe the network administrator entered it directly without revealing the actual password to you.

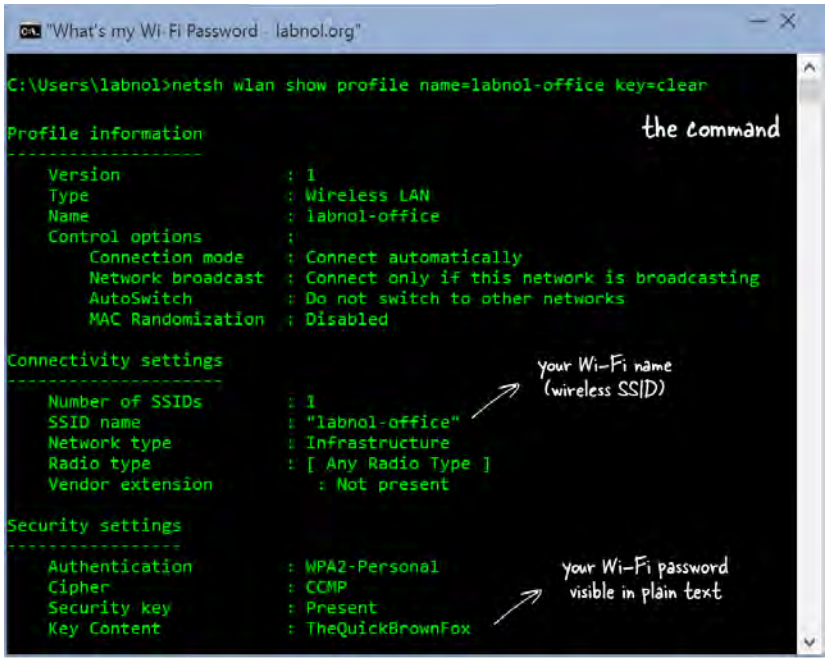
You would now like to connect a second device, like your mobile phone, to the same Wi-Fi network but how do you find out the password? You can either send a password request to the Wi-Fi admin or you can open the command prompt on your computer and retrieve the saved password in one easy step. The technique works on both Mac and Windows PCs.

Find the Wi-Fi Password on Windows

Open the command prompt in administrator mode. Type "cmd" in the Run box, right-click the command prompt icon and choose *Run as Administrator* (see how). Now enter the following command and hit enter to see the Wi-Fi password.

`netsh wlan show profile name=`*`labnol`*` key=clear`

Remember to replace *labnol* with the name of your Wireless SSID (this is the name of the Wi-Fi network that you connect your computer to). The password will show up under the Security Setting section (see screenshot).



If you do not see the password, probably you've not opened the command prompt window as administrator

Start WLAN AutoConfig (Wlansvc Service)

If you are using this technique to retrieve the WiFi password on a Windows computer but getting an error that says – "The Wireless AutoConfig Service (wlansvc) is not running" – here's a simple fix:

Click the Windows Start button and type "services.msc" in the Run box to access Windows Services. Here, go to the WLAN Autoconfig service and make sure that the status is Running. Else, right-click the WLAN AutoConfig service, select Properties and go to Dependencies. Check all the dependencies to make sure they are all running. ☺

Security Terms (Cont. from page 8)

tutorial, though!

Spyware - Focused specifically on gathering information about you. It could be as serious as trying to find out your bank information or as minor as advertisers trying to grab your personal data for targeted ads.

Either way, you might need a special type of security software to take it out. Spybot Search & Destroy does an excellent job of stopping spyware in its tracks.

Keyloggers - A program that copies everything you type and saves it to a file or sends it to the keylogger's owner. Some can even take pictures of your screen or take over your webcam.

Though keyloggers are technically spyware, they're so dangerous they get their own category.

Hackers do use keyloggers, but you're more likely to get one from someone you know. Keyloggers are a favorite of suspicious spouses and significant others. Companies also use them - legally - to check up on employee computer use. ☺

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

Coming Events:

Next Membership Meeting: **1 Aug, beginning at 9 am (see directions below)**
Next Breakfast Meeting: **15 Aug @ 8 am, Country Buffet, 801 N. Academy Blvd.**
Newsletter Deadline: **22 Aug.**

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