PATACS Posts

Newsletter of the Potomac Area Technology and Computer Society

Linux and Open Source News

By Geof Goodrum, Potomac Area Technology and Computer Society
linux(at)patacs.org

Open Source for Canon Digital Cameras

As owner of a Canon "Point and Shoot" (i.e., easy to use consumer model) digital camera, I was happy to discover that camera enthusiasts have developed Open Source software for a variety of Canon camera models, including the Point and Shoot PowerShot Canon models and the high end Digital Single Lens Reflex (DSLR) cameras to give the cameras additional features.

The Canon Hack Development Kit (CHDK, http://chdk.wikia.com/wiki/CHDK) is a software project that supports a long list of Canon PowerShot Point and Shoot models. The CHDK website provides a table of support camera models, links to stable and development versions of the software, and instructions on how to install the software on SD cards. The CHDK software does not replace the camera's internal software (firmware), but loads into the camera memory when the camera starts up with the prepared SD card inserted. The CHDK Wiki lists the following added features, among others:

➢ **RAW** - CHDK can record raw files, giving you access to every bit of data the sensor saw, without compression or processing. Raw files can be manipulated on the camera, or processed on your PC. CHDK supports the open DNG raw standard.

➢ **Override Camera parameters** - Exposures from 2048s to 1/60,000s with flash sync. Full manual or priority control over exposure, aperture, ISO and focus.

➢ **Bracketing** - Bracketing is supported for exposure, aperture, ISO, and even focus.

➢ **Video Overrides** - Control the quality or bitrate of video, or change it on the fly. Extended video clip length - 1 hour or 2GB.

➢ **Scripting** - Control CHDK and camera features using uBASIC and Lua scripts. Enables time lapse, motion detection, advanced bracketing, and much more. Many user-written scripts are available on the forum and wiki.

➢ **Motion detection** - Trigger exposure in response to motion, fast enough to catch lightning.

➢ **Edge overlay** - Detect the edges in a scene, and display them later. Ideal for timelapses, stop-motion, stereography and much more.

➢ **Live Histogram** - CHDK includes a customizable, live histogram display, like those typically found on more expensive cameras. (RGB, blended, luminance and for each RGB channel)

Contents

(Continued from page 1)

- ➢ **Zebra-Mode** - Displays under and overexposure areas live on the screen.

- ➢ **GRIDS** - Create custom grids and display whichever one suits your shooting conditions.

- ➢ **Multi-Lingual Interface** - CHDK supports about 22 languages, and adding more languages is simple.

- ➢ **DOF Calculator** - Display detailed Depth of Field (DOF) information on the screen.

- ➢ **Customizable OSD** - Improved on-screen display of battery status, free space, camera parameters, and much more. Fully customizable with an on-screen editor.

- ➢ **Filebrowser** - Manage files without a PC.

- ➢ **Textreader** - Display text files on your camera.

- ➢ **Games** - Play Reversi, Sokoban, Mastermind, 4-in-a-Row, Tetris, Snake or Sudoku on your camera.

- ➢ **Calendar**

- ➢ **USB Remote** - Simple DIY remote allows you to trigger exposures or scripts.

- ➢ **PTP Extension** - Remote control and display from a PC

- ➢ **Benchmark** - Compare the performance of your SD cards.

- ➢ **User Menu** - Edit your own customizable User-Menu for fast access to often used features.

- ➢ **Battery Indicator** - Always on

- ➢ **Ability to control** dark frame subtraction

Although CHDK stable releases are well-tested and the software does not make permanent changes to the camera, CHDK developers disclaim any responsibility for damages and notes that use of CHDK may void the camera warranty (Canon's responses vary on this point).

Magic Lantern (http://www.magiclantern.fm/) is an Open Source firmware project for Canon Digital Single Lens Reflex (DSLR) cameras used by professionals and serious camera enthusiasts. Some of the models that Magic Lantern supports are: Rebel T1i (500D), T2i (550D), T3i (600D), T4i (650D), T5i (700D) and T3 (1100D); EOS M; 5D; 5D Mark ii; 5D Mark iii; 6D; 7D; 40D; 50D;and 60D. Some of the features noted for Magic Lantern 2.3 are:

- ➢ **Audio** - disable AGC, audio meters, manual audio controls, selectable input source (internal, internal+external, external stereo, balanced), audio monitoring via A/V cable.

- ➢ **Exposure helpers** - zebras, false color, histogram, waveform, spotmeter, vectorscope.

- ➢ **Focus tools** - focus peaking, zoom while recording, trap focus, rack_focus, follow_focus, stack_focus.

- ➢ **Movie helpers** - Bitrate control, movie logging (Exif-like metadata), auto-restart after buffer overflow or 4 GB limit, HDR video, advanced FPS control.

- ➢ **LiveView adjustments** - contrast, saturation, display gain for using LiveView in darkness.

- ➢ **Cropmark images** - user-editable overlays to assist framing and composition.

- ➢ **Fine control** for ISO, Shutter, Kelvin white balance and other image settings.

- ➢ **Bracketing** - advanced exposure bracketing, focus stacking.

- ➢ **Remote release** with LCD face sensor and audio trigger, without extra hardware.

- ➢ **Timelapse** - intervalometer (for photos and movies), bulb ramping (manual and automatic), recording at very low FPS (down to 0.2 FPS), silent pictures without shutter actuation.

- ➢ **Astro and night photography** - bulb timer for very long exposures (up to 8h).

- ➢ **Info displays** - focus and DOF info, CMOS temperature, shutter count, clock.

- ➢ **For strobists** - flash exposure compensation, range up to -10 to +3 EV (depends on the camera).

- ➢ **Power saving** - Turn off display or reduce **backlight** in LiveView during idle times.

- ➢ **Handy features** - Quick zoom in PLAY mode, key shortcuts for **commonly**-used features, customizable menus.

In July 2013, one of the lead Magic Lantern developers, A1ex, announced in a forum post (http://www.magiclantern.fm/forum/index.php?topic=7139.0) a software module to add a "Dual ISO" mode to the 5D Mark iii and 7D models.

(Continued from page 2)

While the cameras have built-in modes to produce High Dynamic Range (HDR) images and video, the Dual ISO mode eliminates motion artifacts by sampling half of the sensor at ISO 100 and half at ISO 1600 in a single image. The end result is an image (or video) with extremely wide dynamic range, with the result that bright light does not wash out details in darker areas of the image.
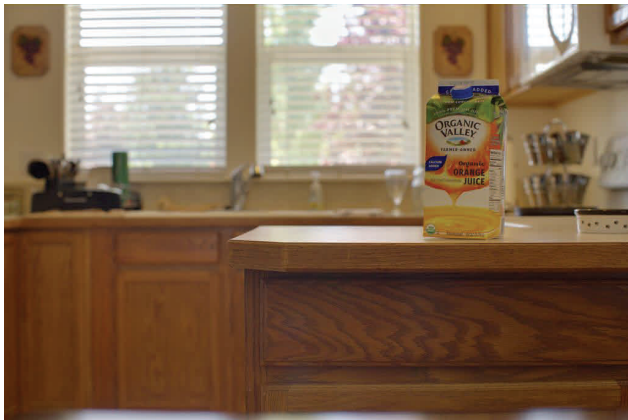
This image included in the original forum posting (http://acoutts.com/a1ex/0R0A0640-fullres-soft.jpg) shows how the details of the foreground are preserved even with a bright window in the background. There is a PDF linked in the posting that details how the process works. Other postings by forum members include more image samples and indicate some artifacts and limitations in this feature. However, the overall reception has been enthusiastic, and the implementation continues to improve.

Magic Lantern includes similar disclaimers to CHDK.

I found references to similar efforts to create custom firmware for Nikon cameras (e.g. http://nikonhacker.com/), but Canon seems to have the lead in community-developed software.

Featured Open Source Software of the Month October 2013

The software described below can be downloaded at the links provided or copied onto a USB flash drive at the PATACS Fairfax meeting. However, please check the online package management tool included with your GNU/Linux distribution first, as installation is often just a click away.

Blocks of the Undead – v1.0.
http://www.gamecreation.org/game/blocksundead .
Free GNU General Public License source code and Debian executable package by Jared Luxenberg, Justin Lokey, Keith Bare, and Korina Loumidi. A falling block puzzle game with a spooky theme. The objective is to clear all the blocks on the playing field. Blocks are cleared when there are three of them (or more) in a row. Also, "L-shaped" patterns can be formed, and all the blocks in the L will be cleared. Move the white cursor around on the playing field by moving the mouse, and click to swap the two blocks under the cursor. Press escape to exit, your progress will be saved. There are three stages, each with six levels. *Good luck!*

Requires SDL 1.2 media libraries, included with most distributions.

Screenshot link:

http://stage.gamecreation.org/blocksundead/images/blocksundead-2.jpg

SDL – v2.0.0. http://www.libsdl.org/
Free zlib license source code for Microsoft Windows, Apple Mac OS X and iOS, Linux, and Google Android by Sam Lantinga and the SDL community. Support for other platforms may be found in the source code. Simple DirectMedia Layer is a cross-platform development library designed to provide low level access to audio, keyboard, mouse, joystick, and graphics hardware via OpenGL and Direct3D. It is used by video playback software, emulators, and popular games including Valve's award winning catalog and many Humble Bundle games. SDL is written in C, works natively with C++, and there are bindings available for several other languages, including C# and Python. SDL 2.0 is a major update to the SDL 1.2 codebase with a different, not backwards-compatible API. It replaces several parts of the 1.2 API with more general support for multiple input and output options. Some feature additions include multiple window support, hardware-accelerated 2D graphics, and better Unicode support.

TeXstudio – v2.6.2.
http://texstudio.sourceforge.net/
Free GNU General Public License source code and executable packages for Arch, CentOS, Fedora, Debian, Ubuntu, and openSuSE by Benito van der Zander, Jan Sundermeyer, Daniel Braun, and Tim

Useful Bits & Pieces
October 2013
By Lorrin R. Garson, PATACS

Disasters Aplenty

Do you relish up-to-date information on earthquakes, tsunamis, hurricanes, volcanoes, landslides, fires or severe weather? Consider installing Earth Alerts from http://earthalerts.manyjourneys.com/
You may also be interested in Google's Earth Alerts Beta at http://earthalerts.manyjourneys.com/web/

Temporary E-Mail Address

At times you may need a temporary e-mail address. Often a 10-20 minute e-mail address will do, such as "10 Minute Mail" at
http://10minutemail.com/10MinuteMail/index.html
On other occasions you may need a temporary e-mail address for days or a few weeks. Consider using TrashMail.net at https://ssl.trashmail.net/?lang=en
This free service provides the following:

➢ A randomly chosen temporary e-mail address or an e-mail address you make up.

➢ Your choice of 1 to 10 e-mail messages that will be forwarded to your "normal" e-mail address.

➢ Your selection of the period the temporary e-mail address will be active: 1-6 days, or 1-3 weeks, or 1 month.

➢ Once either (a) the number of e-mail messages to be forwarded or (b) the time period has been exceeded, the temporary 2-mail address is eliminated.

Since your temporary e-mail address will be in the form Something@trashmail.net, if you are making this available to a person you will probably want to explain that this is a temporary e-mail address and messages sent to that address will be forwarded to your private e-mail address for a limited period of time.

More flexibility and options are available for $12.99/year.

Xinorbis Analyzer

This free utility is a powerful hard disk analyzer that presents information in a variety of ways (graphs, tables, tree displays, etc.). It can be used to analyze a single drive as well as specific directories. Xinorbis can be complex but provides much useful detailed information.   There is a 73-page pdf manual available that can be downloaded. The application can be downloaded from
http://www.xinorbis.com/xinorbis/

Start Menu for Windows 8

It seems that Microsoft is going to bring back the Start Button in Windows 8.1, well not quite. Various reports suggest that it won't be the Start Button of old (à la Windows 7 and earlier versions) but rather a shortcut to Win 8's Start Menu. Those using Windows 8 may still wish to use an alternative.   In Table 1 below are eleven possibilities. For more details see *MaximumPC*, September 2013, pp. 52-56.

New Nexus 7 Tablet

Google has unveiled a new version of its budget-priced Nexus 7 tablet. The new device has 1080p resolution (1920 x 1200) with 7-inch display (hence the name Nexus 7). The new model is thinner, weighs 0.64 lbs. and boasts a 1.5 GHz quad-core CPU running the Android 4.3 OS. Battery life is expected to be improved. Built-in speakers emulate 5.1 surround sound. The device has a 5-megapixel rear-facing camera. The price has risen from$199 to $229 for the 16 GB model. The 32 GB model is priced at $269.

Store Your Keys in the Cloud

Are you concerned about losing your house keys? Calling a locksmith can be expensive. Here's a solution… store your keys in the Cloud! Huh, you're thinking? Yes, in the Cloud. KeyMe is an app for iPhones, iPads, and iPod Touch. This app allows you to take a photo of your keys, store then in the Cloud from which a physical copy of your keys can be made. A locksmith can make a key by viewing the instructions displayed on your iDevice. The app

(Continued from page 4)

is free as is the storage of any number of keys, but of course you have to pay for keys. Keys can also be ordered via Mail Order. See https://www.keyme.net/ for information. Regarding security, "We do not store information which could be used to link your key with a location or lock. We don't know where you live and we don't want to know."

A Faster Internet

TCP (Transmission Control Protocol) is a set of rules that govern the way data moves around the Internet. Data are broken down into packets that often take different routes to their destination and then get reassembled. TCP was designed to be sure data arrive accurately and complete, not necessarily in the fastest way. Researchers at MIT have developed a system called Remy that enhances TCP by improving routing of the packets. Will this technology become widely deployed? Perhaps. See http://web.mit.edu/remy/
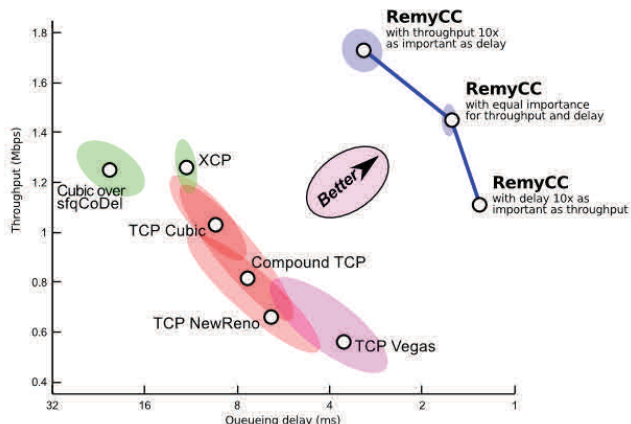
Table 1: Start Button Alternatives for Win 8				
Name	**Access**	**Price**	**Comments**
Classic Shell	http://www.classicsshell.net/	Free	Able to ignore Modern completely. Highly customizable "Modern" is the name Microsoft gives to the Windows 8 user interface. It was formerly called "Metro".
Pokki	http://www.pokki.com/	Free	Frustrating installation. May not work with 64-bit Windows 8
Power 8	https://code.google.com/p/power8/	Free	Disables Modern's Hot Corners
RetroUI Pro	http://retroui.com/	$4.95 or 3 PCs for $9.95	A bit clumsy to use
StartMenu7	http://www.startmenu7.com/index.html	Free	All programs in a single large menu
Start Menu Reviver	http://www.reviversoft.com/	Free	Numerous links and shortcuts. Limited configuration options
Start8	http://www.stardock.com/products/start8/	$4.99	Very Windows-7 like
StartIsBack	http://www.startisback.com/	$3.00 for 2 PCs	Windows-7 like
StartMenuPlus8	http://www.winok-msixray.com/	$4.99	Mixed reviews
StartW8	http://www.areaguard.com/startw8	Free	Simple and easy to use
ViStart 8	http://lee-soft.com/vistart/	Free	Reasonably configurable

DHS, FBI, Warn About Threats to Android Mobile Devices

By Ira Wilsker

Websites

http://publicintelligence.net/dhs-fbi-android-threats/
http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf
https://en.wikipedia.org/wiki/Android_(operating_system)
http://www.techsupportalert.com/content/best-free-antivirus-app-android.htm
https://play.google.com/store/apps/details?id=com.qihoo.security
http://play.google.com/store/apps/details?id=com.trustgo.mobile.security
https://en.wikipedia.org/wiki/Carrier_IQ
http://money.cnn.com/2011/12/01/technology/carrier_iq/index.htm
http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/
http://www.youtube.com/watch?feature=player_embedded&v=T17XQI_AYNo

In a document labeled "U//FOUO (Unclassified For Official Use Only) Roll Call Release for Police, Fire, EMS and Security Personnel", dated July 23, 2013 the Department of Homeland Security (DHS) and the FBI issued a warning about security threats to Android powered mobile devices.

According to recently published industry figures, mobile devices powered by Google's Android operating system currently comprise about 75% of all mobile smart devices, making Android the world's most widely used mobile operating system. Even though Google designed Android to be secure, and have each running "app" or program run in a closed memory space or "sandbox" in order to protect one bad app from infecting the entire device, Android devices have become a primary target for malware authors. Because the Android operating system is released as "open source", and the program has much in common with the well known Java operating system, Android has become the targeted operating system of choice for creators of malware.

While Google has frequently released updates and upgrades to Android, many of which have improved and increased the security of the operating system, 44% of Android users are still using the out-of-date (2011) "Gingerbread" or versions 2.3.3 to 2.3.7 of the operating system. These older versions of Android, which were once thought to be secure, are now known to have several known security vulnerabilities; Google repaired and patched these vulnerabilities in later versions of Android. In this "Roll Call Release", the DHS and FBI warned that "The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date." It only seems logical that this warning would equally apply to privately owned Android devices as well. Personally, as the owner of several Android powered mobile devices, I can attest to the fact that many of the "older" Android devices running some form of Gingerbread, many of which are still currently available in the marketplace as "new" devices, cannot be readily upgraded to the newer versions of Android. The latest version of Android released by Google is "Jelly Bean", a tweak to version 4.3, released on August 23, 2013. It is important that, in terms of security, the latest Android updates available be installed and updated again as appropriate.

According to this DHS-FBI warning, there are three primary security threat types currently targeting mobile devices running the Android operating system. Almost one-half of the current threats are called "SMS (Text Messaging) Trojans". Targeting

(U) Malware Threats to Mobile Operating Systems, 2012

UNCLASSIFIED
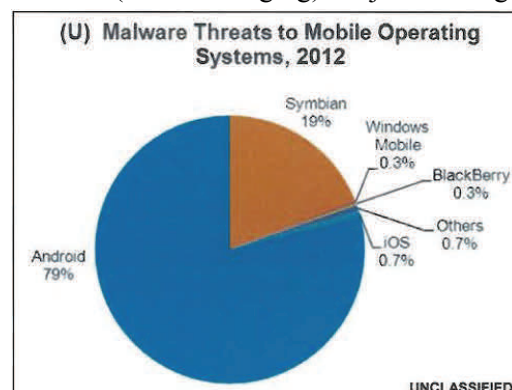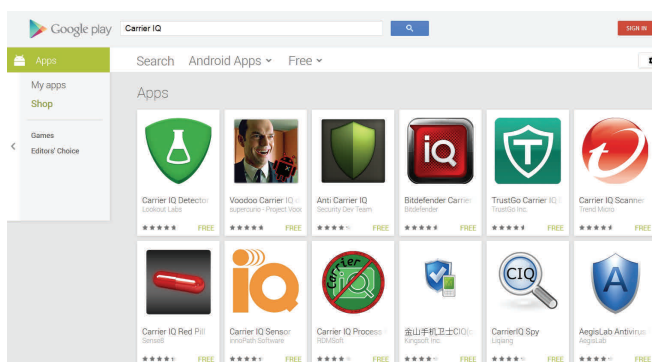
(Continued from page 6)

predominately the older, unpatched versions of Android, such as Gingerbread, these trojans send text messages, unknown by the user, to premium rate numbers owned or operated by the hackers; these financial charges, often unreasonably high, appear on the monthly bills of the victim user, with the bulk of the proceeds going to the criminal enterprise. While Android devices are essentially immune from traditional computer viruses, the DHS-FBI warning suggests that this threat can be reduced with the simple installation of a comprehensive security app. While almost all of the commercial security software companies offer a paid Android security suite, there are also several excellent Android security suites available for free. An updated list (revised August 8) of the top rated free Android security suites is available from Gizmo's TechSupportAlert.com at www.techsupportalert.com/content/best-free-antivirus-app-android.htm. According to the Gizmo reviews, the current top-rated free Android security suite is 360 Mobile Security - Antivirus by Qihu Software, closely followed by what I have on my personal Android phone, TrustGo Antivirus & Mobile Security. These, and all of the other free security suites listed by Gizmo are available from the Google Play Store, accessible directly through the device, or from Android web store at play.google.com.

The second major type of threat to Android powered devices are generically called "Rootkits", which are a type of malware that hides itself from traditional forms of detection. In 2011, a controversial rootkit, that had likely been intentionally installed on the phone by its manufacturer or carrier, was found to be running on

millions of mobile devices. According to Wikipedia (en.wikipedia.org/wiki/Carrier_IQ), an intentionally installed rootkit, Carrier IQ, has been installed on over 150 million Android phones. Wikipedia says that Carrier IQ, "is software, typically pre-installed on mobile devices by handset manufacturers or network operators, designed to gather, store and forward diagnostic measurements on their behalf. Data available can include metrics on the device itself (e.g., firmware, battery levels, application performance, web performance) and performance data on voice and data connectivity between the device and radio towers."

While this may seem innocent enough, as the phone carriers need to monitor system performance, there is also substantial evidence that this Carrier IQ software "phones home" with a lot more than basic performance information. On December 1, 2011, CNN broke the story "Carrier IQ: Your phone's secret recording device" (money.cnn.com/2011/12/01/technology/carrier_iq/index.htm). According to the CNN report, "Carrier IQ is a piece of software installed on millions of mobile phones that logs everything their users do, from what websites they browse to what their text messages say." CNN was referring to an earlier study by Android expert Trevor Eckhart who first published concerns that Carrier IQ was transmitting more than just system data, followed up by a YouTube video (http://youtu.be/T17XQI_AYNo) detailing the personal data being captured and sent to the carriers. In his YouTube video, Trevor Eckhart showed how the Carrier IQ software factory installed on his Android phone recorded every key stroke, every text message, and the URL (internet address) of every website that he visited, including websites that are encrypted to prevent tracking. Immediately following the CNN report, the publisher of Carrier IQ announced, "While a few individuals have identified that there is a great deal of information available to the Carrier IQ software inside the handset, our software does not record, store or

Best Free Security Apps for Android - Feature Comparison Chart

		Secure Browsing	Privacy Advisor	SPAM SMS Filter	PUA Detection	Anti-theft	Call & SMS Filter	USSD Protection	Backup & Restore	RAM Friendly
1	360 Mobile Security - Antivirus	✗	✓	✗	✓	✗	✗	✗	✗	✓
2	TrustGo Antivirus & Mobile Security	✓	✓	✗	✓	Web-based	✗	✓	✓	✓
3	Avast! Mobile Security	✓	✓	✓	✓	Web & SMS	✓	✓	✗	✗
4	Lookout Mobile Security	✗	✗	✗	✓	WEB (Device Location)	✗	✓	Just Contacts	✗
5	Comodo Mobile Security & Antivirus	✓	✓	✓	✓	SMS-based	✓	✓	✓	⟳
6	Zoner Antivirus Free	✗	✓	✗	✓	SMS-based	✓	✗	✗	⟳
7	Sophos Security & Antivirus	✓	✓	✗	✓	SMS-based	✗	✓	✗	✓
8	Dr. Antivirus Light	✗	✗	✗	✓	✗	✗	✗	✗	✓
9	AVG Antivirus Free	✓	✗	✗	✓	Web-based	✗	✗	✗	⟳

Legend:
✓ The app includes this feature in full
✗ Not at all
⟳ Variable performance

(Continued from page 7)

transmit the contents of SMS messages, email, photographs, audio or video." (Wikipedia).

There are several free (and paid) Android apps in the Google Play Store that can detect Carrier IQ, and notify the user of its presence; simply search the Google Play Store (play.google.com) for "Carrier IQ". While it is free and simple to detect the Carrier IQ rootkit software on Android phones, it is extremely difficult to remove, with some published reports that many phones that have had the Carrier IQ software removed lost functionality, and were no longer covered by warranty (source: Wikipedia). There are also some apps that can cripple some of the Carrier IQ reporting, without actually removing it from the phone. The

DHS-FBI warning recommends that Android devices used by first responders should have Carrier IQ removed. For the record, all of my Android devices tested positive for the Carrier IQ software.

The third security threat mentioned was "Fake Google Play Domains". These websites were created by cyber crooks to trick innocent users into downloading and installing malicious apps. These malicious apps, which often appear as legitimate music, books, magazines, movies, TV programs, and other applications, are designed to steal sensitive information, financial data, user names, and passwords. While not perfect, as some malicious apps have been slipped through and been posted, the genuine Google Play Store (play.google.com) is probably the safest resource for Android apps. The DHS-FBI warning also advises that security software, such as some of those mentioned above, should be installed on the Android devices and frequently updated. If any malicious software is found, it should be removed immediately, followed by an immediate change in any possibly compromised user names and passwords.

If the Department of Homeland Security (DHS) and the FBI believe that the security threat to Android devices is serious enough to post a "Roll Call" message to first responders, perhaps the same warnings should be considered by private citizens.

Just in case that Apple iOS device users think that their smart devices are immune from security threats, do not be complacent; your devices are at risk as well.

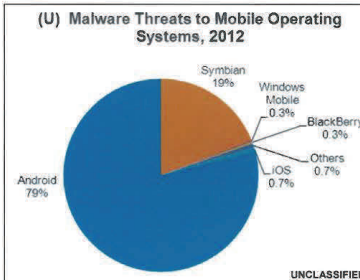UNCLASSIFIED//FOR OFFICIAL USE ONLY

ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

23 July 2013

(U//FOUO) Threats to Mobile Devices Using the Android Operating System

(U//FOUO) Android is the world's most widely used mobile operating system (OS) and continues to be a primary target for malware attacks due to its market share and open source architecture. Industry reporting indicates 44 percent of Android users are still using versions 2.3.3 through 2.3.7—known as Gingerbread—which were released in 2011 and have a number of security vulnerabilities that were fixed in later versions. The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date. The following are some known security threats to mobile OS and mitigation steps.

(U) Malware Threats to Mobile Operating Systems, 2012

Android 79%, Symbian 19%, Windows Mobile 0.3%, BlackBerry 0.3%, iOS 0.7%, Others 0.7%

UNCLASSIFIED

Security Threat	Description	Mitigation Strategy
SMS (Text Message) Trojans represent nearly half of the malicious applications circulating today on older Android OS.	Sends text messages to premium-rate numbers owned by criminal hackers without the user's knowledge, potentially resulting in exorbitant charges for the user.	Install an Android security suite designed to combat these threats. These security suites can be purchased or downloaded free from the Internet.
Rootkits are malware that hide their existence from normal forms of detection. In late 2011, a software developer's rootkit was discovered running on millions of mobile devices.	Logs the user's locations, keystrokes, and passwords without the user's knowledge.	Install the Carrier IQ Test—a free application that can detect and remove the malicious software.
Fake Google Play Domains are sites created by cybercriminals. Google Play enables users to browse and download music, books, magazines, movies, television programs, and other applications.	Tricks users into installing malicious applications that enable malicious actors to steal sensitive information, including financial data and log-in credentials.	Install only approved applications and follow IT department procedures to update devices' OS. Users should install and regularly update antivirus software for Android devices to detect and remove any malicious applications.

UNCLASSIFIED

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0166-13

(U) Prepared by the Office of Intelligence and Analysis, Cyber Intelligence Analysis Division, and the National Protection and Programs Directorate, US Computer Emergency Readiness Team. Coordinated with the FBI, Directorate of Intelligence. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Customizing the Ribbon in Office 2010

Nancy DeMarte, Regular Columnist (Office Talk), Sarasota PCUG, Florida

If you are a Microsoft Office user, by now you have probably experienced the "ribbon." Introduced with Office 2007, the ribbon was a radical change in the way commands were displayed in the Office programs, such as Word, PowerPoint, and Excel. In previous versions, "drop down menus" were the norm. You clicked a term on the menu bar, and a list of clickable commands slid down the page. Beginning with Office 2007, commands were lined up across the top of the screen, organized by tabs in a ribbon-like structure. Each tab contained "groups" of similar commands. Needless to say, the new ribbon met with much resistance. There was no way to revert to the earlier look or to customize the ribbon. All a user could do was minimize the ribbon by double-clicking any tab or add and delete items from the Quick Access bar above the ribbon.

Microsoft got the message. When Office 2010 was released, one of the categories in the Options sections of each program was "Customize Ribbon." Users could create new tabs and fill them with groups of any commands they chose. They could hide any or all tabs, rename them, save their customized ribbon, and export it to other computers. Customization of the ribbon was easy; it was all done in a single window.

Opening Word 2010, because I use it often, I set out to customize the ribbon. I found that, although the default commands could not be renamed, reordered or deleted, I could add new custom tabs and groups. So I decided to create a tab called Newsletter, into which I would put some groups of commands that I use when composing newsletters. First I opened the Customize the Ribbon window (File / Options / Customize Ribbon.) I soon learned that the quicker way was to right click any default tab on the ribbon and then click, Customize the Ribbon. Then I added a new tab (New
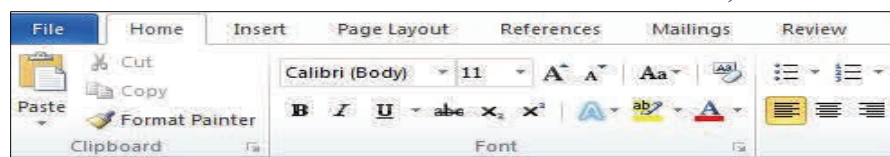
Tab button - OK), which also added a new unnamed group. Both my tab and group had the word "custom" after them, but I found this word is not visible on the actual ribbon. Then I renamed my tab (Select the tab - Rename button - typed *Newsletter* – OK). If I had changed my mind and wanted to delete my new tab, I could have right clicked it and selected Remove at any time.
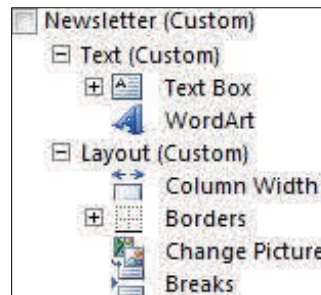
Then I created another new group on the tab, using the same steps as I had used for creating a new tab. I clicked each new group, selected Rename, and typed *Text* and *Layout*. Then it was time for the hardest part – choosing the commands I wanted to add to the groups. Office programs contain hundreds of commands, many of which do not appear on the default ribbon. First I spent time scrolling through the Popular and All Commands lists in the left pane, where I found a few that fit my needs. I clicked Text group in the right pane, then the command name in the left pane, and then the Add button between the panes. I repeated this process to add the rest of the commands I wanted, looking in other lists, including "Commands not in the ribbon." When I renamed the first command, I found I could attach an icon to it from a gallery which opened next to the renaming box. I repeated these steps for the remaining tab and commands. Now when I open Word 2010, my Newsletter tab appears along with the default tabs. When writing a newsletter, I can stay on that tab most of the time. If later I want to get rid of it, I can go to the Customize the Ribbon window, right click each item and click Remove or choose to Reset the ribbon to its original state. Note: Resetting also removes all customizations of the Quick Access bar.

Some Tips About Customizing The Ribbon

1) Since the ribbons on the Office 2010 programs each have different tabs, groups, and commands, customizations only apply to the program in which they are created.

2) You can't delete a default tab in Office 2010, but you can hide it by unchecking the box next to the tab name in the Customize the Ribbon window.

3) You can export your customized ribbon to another computer by saving it as a file and exporting it. In the Customize the Ribbon window, click Export/Import. Click "Export all customizations." Then go to the computer which is to receive the file, open the customization window and click "Import customization file." Caution: This will replace any customizations that have been done to that program on the receiving computer.

4) The ribbon is now being used by Microsoft in many venues, including Windows 8. In Office 2013, the ribbon can be customized in the same way as Office 2010.

5) It is easy to minimize the ribbon in Office 2010, leaving only the tabs. Click the tiny up arrow to the left of the Help icon near the right end of the ribbon. Minimizing the ribbon opens up more work space in the program window. Click it again to restore the full ribbon.

6) If you need help with the ribbon, click the Help icon (?) in the top right corner of any Office window and search for "Office ribbon customization."

Windows 8: Big Differences From Win7, And It Works!

By Karen Stagg,
Member, Golden Gate Computer Society
March 2012 issue, GGCS newsletter
www.ggcs.org/ **editor (at) ggcs.org**

Windows 8 is substantially different from previous versions of Windows, and, though it requires a learning curve, the task is not insurmountable, says GGCS member Ernie Ganas, who helped about 75 guests and members understand the newest Microsoft operating system (OS) during the February General Meeting.

To make the newness more palatable, Ernie offered that this new OS takes only 15 to 20 seconds to boot and 10 seconds to shut down. And the Internet loads instantly.

In addition, Windows 8, which costs about $200, is a stable platform—more so than previous versions of Windows, which has been a concern since even-

numbered Windows upgrades have notoriously had problems in the past. Windows Defender is standard in Windows 8 and replaces Microsoft Security Essentials.

The online app store for Windows 8 has 35,000 choices to purchase online, though many are free. The term "apps" is starting to replace the word "programs" but can still be used interchangeably.

Be aware that many of the default applications or preferences are made by Microsoft, i.e. Bing instead of Google. If you don't like Bing, you can choose Google (or another search engine), and Lock your choice in Internet Options>Tools.

Windows 8's (Pro version or higher) unique feature called "Windows to Go" (WTG) allows you to boot your workspace from a USB flash drive, so you can see your desktop as you would see it at home—your files, programs, etc.—on any computer you plug into. If you need to use someone else's computer, say, while traveling, WTG builds a virtual box that holds your Windows environment. Your information is never on that computer; it's all just on your flash drive.

The logon screen, though inconvenient to some, does serve a purpose. It allows a user to sign into a different computer and have their home configuration (including references) visible.

Windows 8 also helps us access our data by promoting the use of cloud storage with Sky Drive, available in various size options. Ernie suggests that the trend in computer security may be to virtual environments to protect computers better.

How It Looks and Works

The new Task Manager is well-designed, showing useful information not available with previous Windows versions. The initial start-up screen shows many icons such as:

➢ Weather
➢ Maps
➢ People
➢ Mail
➢ Games

But the "search" feature is the fastest way to find anything (apps, settings or files) on your Windows 8 computer, Ernie says.

(Continued from page 10)

Windows 8 stores your data in a "pool." It gathers files and data from multiple sources such as your flash drives, hard drives, or other storage mediums. The only drawback is that once the data is transferred to the pool, you can no longer determine from what device the information was transferred from.

Windows 8 was made to be used with a touch screen monitor, but those of us (the majority attending the meeting) still have the conventional screens and can handily navigate Win 8 with a mouse or touchpad.

To return to the "Tiles" view, use the Windows key on the keyboard. To close a tile, the screen offers no obvious place to click Close. Instead, for those with a touchscreen, hold your finger at the top of the screen and "brush" the screen down or toward you, as if you were brushing something off the screen itself. To do this action with a mouse, click and hold at the top of the screen, then drag the window down instead of "brushing" it. Old timers remember the Alt + F4 keystroke works too.

Users with touchscreen experience on an iPhone or Android, iPad or, tablet will be familiar with "brushing" or "sliding" motions. Ernie speculates that the computer industry is headed toward a tablet/phone touchscreen interface.

The touchscreen and decidedly visual platform isn't intuitive. Ernie's first challenge was figuring out how to start, restart, and shut down—he found no button in an obvious place. Windows 8 does offer some right-click options for shut down and closing a window. Finding them is another matter. In addition, Ctrl + Alt + Delete doesn't work in this version of Windows.

John King, one of our well-schooled computer buffs, responded to Ernie's request for an experienced assessment of this new system: "It is a stretch to learn this system." Fortunately, the Microsoft store in Corte Madera is well set-up for customers to learn how to use all the bells and whistles in their products. Ernie suggests YouTube as a valuable source for tutorials.
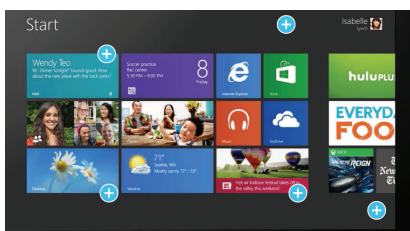
Windows 8 Corner

By Rosita Herrick, Member, Sarasota PCUG, Florida

The Store App

One of the Apps (applications) distributed with Windows 8 is the Store application as shown below.

There are over 100 free Apps available for download including games, productivity and utility Apps like U-tube Downloader, Windows 8 Tool Box etc.

When you click on the Store app, you will see three tiles titled: Top Paid, Top Free and New Releases. Clicking on any of these tiles will open a full screen with names, (prices if any) and description.

Installing an App from the Microsoft store is easy. If the App is free, just click on the install box and in less than a minute it is installed and available for access. If the App is not free, you can download it for a free trial or pay using your Microsoft account.

Uninstalling an App is just as easy. On the Start Screen, right click on the App. At the bottom of the screen, a bar with 6 icons is displayed. Just click on the Uninstall icon and it will be uninstalled and removed from your PC.

If you are curious why the number 1 is displayed on the Store App tile, it is because on one of the Apps I downloaded it has an available update. When I click on the Store tile, the Update link is displayed on the upper right corner.

A click on the link will show the name of the App (in this case Utube Player/Downloader) and at the bottom of the screen will be the option to install the update.
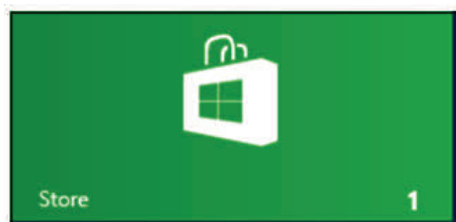
Organizing and Backing Up

By Diane Fahlbusch, President, ICON PC User Group, Long Island, NY

February 2013 issue, The ICONPCUG Graphic
www.iconpcug.org editor (at) iconpcug.org

We all have LOTS of files saved to our computers as well as on other hardware, such as MP3 players, camera cards, thumb drives and CDs/DVDs, and the cloud. The problem with having lots of hard drive space and cheap mass media storage is that, well, we use them…a LOT, and often store way too much. The first problem is finding the files you want quickly when you want them amidst all that you have. Think about this:

Why did I create and save this file?

Wow! I have this?! I was just playing. It had a purpose once upon a time. It has nifty information. It saves me from looking it up again. It's a wonderful trip down memory lane. I really wanted it! I use it frequently. I need it for work. It's precious to ME. It's precious to me AND others. It's important stuff. I need it for work or a specific project. It's legally required.

Only you can determine how important your files are, but start rethinking what you save in the first place.

The second problem is what happens if you lose this file. Here are some things to consider:

What will your reaction be?

None because you forgot it was there. Say "So what". Pout for a few minutes. Cry for a few hours. Lose a night's sleep. Have a panic attack until I figure out how to rectify it. Curl up in a fetal position for numerous days. Take a sudden trip to the ICU ward of your local hospital.

What would I do if I lost it?

Not even realize it's gone. Say "Oops" and forget about it. Recreate it easily. Spend a lot of time recreating it. Spend more money to get another copy. Be unable to recreate it. Lose your job or spouse. Be in potential legal trouble.

If you are the beginning point in the scale, you REALLY need to clean out files. If you are on the later end of the scale, you REALLY need a Backup plan. But do you just want to duplicate that big messy "pile"? So it's time for:

Organization

Files are useless if you can't find them when you need them. You first must get in the habit of using meaningful names for your files, and try to keep them short. Advanced search options do allow you to search for a word or phrase in the document and on your entire hard drive. But that can be time consuming. The programs we use want to save files where the programmers decided to set up as the default location. YOU need to take control of this by remembering to select the "Save" location or you are at their mercy. (Of course, it helps if you had initially set up some organization prior to doing this. However, you can still do it after the fact.)

It's up to you how you want to organize your folders and files. One of the best ways to think about how to organize them is by considering how you would do it if they were all paper documents. Most people would get a filing cabinet and use some kind of system, such as tax returns in one sections, legal certificates in another but fairly close, other legal documents, banking, etc. Well, do that with your electronic files. Create folders and subfolders. If you use specific programs for your banking, you can create shortcuts to the programs within the folders. You may need to add even more layers, but don't be excessive. If you maintain important documents such as tax records, I would suggest that you create folders for these that are separate from the remainder of your documents, or not even store them on your computer at all.

Most of your document files wind up in the "My Documents" folder on your Windows machine. Most programs will separate out your photos, music and videos into the "My" files of coordinating names, or in a subfolder within the specific program's folders. The problem is that hackers and phishers know where to look for these files. You should get into the habit of creating your own folders, just as you did when everything was kept in file boxes or filing cabinets. Keep sensitive information encrypted and in folders OUTSIDE of the "My Documents folder".

Once you have created your filing system, it's time for the work of going through your files to make sure they still open—otherwise, why save it? Next, ascertain whether you still want or need them. One question you can ask yourself is, "Did I actually remember that I

had this?" If the answer is "No", then you might want to get rid of it. (That's the problem with LOTS of hard drive space – we don't get rid of anything.) Another option is to consolidate related information onto one file. (I know I started numerous documents with tips about a specific program, which I eventually just put into one document.) Depending upon how many you have, I suggest that you attack it a little at a time. You may find that you need to create more folders to accommodate the information you have accumulated.

While you are moving and checking your files, you might want to consider adding some "mouse over" information. RIGHT click the file, and then click on "Properties". You can add comments, keywords, etc. Unfortunately, most of us do not do this. This can become very handy if you need to have the same file in multiple locations. Now you can note how many copies there are and where they are. Photos often require you to put this information in your metadata. There are programs that can help you do this, but most of the time the metadata is editable through your camera's software. There are often batch renaming options included with this software, as well as other programs. Don't forget to add notations about the people and places in those photos, especially if you want to share them with future generations. Now you understand what programmers mean by "document, document, document"!

Additionally or as an alternative, you could use Microsoft's One Note to create electronic loose leaf binders of information that can help pull information together. Or you could create links to your folders and use the program Fences to keep them grouped and hidden until you want them. Or you could actually create a database that can contain even more information and hyperlinks to your documents so they are but a click away. Use what works for YOU. But it still makes sense to create order and KEEP IT THAT WAY.

So you have slogged through all of your files scattered throughout the universe, created order from chaos, and provided possible cross-references and information. Great! But what happens if that drive dies? That's why you need a:

Back Up Plan

The first step is making sure you have a physical medium to back up to. CDs and DVDs are quick and cheap, and there are lots of free burning programs, but they are usually not recommended, even by their manufacturers, for long term archiving of data. Thumb drives are a better option, but are also known to go bad, and do have a limited number of times they can be rewritten. (Granted, it's a huge number, so you may want to keep a drive just for backups.) Hard drives provide the greatest longevity, and the old fashioned magnetic discs are recommended for the long haul. Of course, they can lose the data if they cross paths with a magnet. That's why you should have at least two sets. Yep, the ol' duplicate backup motif.

However, the aftermath of Super-storm Sandy, and her kin in other areas, proves that even if you backed up to multiple drives, they would all be lost if they are saved in the same building. Back up physically to multiple sources, and at least one site away from where your main stockpile of data is stored. This includes the cloud, or another hard drive in a safe deposit box. Why a safe deposit box? Because of the way banks are built, they will survive most natural disasters. Also consider keeping your backup drives in a refrigerator. If you can get your hands on one of those small ones that college kids use, even if it is not running. We don't want to keep the drives chilled; we just want to protect them from fire. (The insulation in your refrigerator, but especially the freezer, is so thick that items such as these would survive a fire that destroys the entire house.) You could use one of those locking fire proof boxes, except that most thieves just grab the whole box … but not the icebox.

Now it's time to back up. You can just simply copy files, especially those important, costly or irreplaceable ones, to another drive, and another. But please remember that certain files may only be opened with a specific program. Look into alternative programs that might be able to import the file. (The open source Open Office and Libre Office both have a word processing program that will open most forms of MS Word documents. You may lose some formatting, but the text will be there.) Consider saving files with formats that can be opened by other programs without imports or conversions (.odt, .pdf or .txt). Of course, regular backups are a must.

Another alternative, especially if you have a lot of files that you want to save and are always editing them or adding new ones, but forget to back up our files is to build yourself a NAS (Network Attached

(Continued from page 13)

Storage device). Yes, you can buy them but you can also take an old computer and build one with the cross platform open source Free NAS. Your data will be backed up as you are working on it. This will also back up your entire system if you want it to.

Another choice is to use software specifically designed to use backups. Yes, all of the Windows operating systems from at least '98 had this. The problem is that you need to restore your backups with the same operating system. So if you backed up files in the Windows XP backup THAT is the OS you will need to be using to restore them.

Of course you can always look for third party software to backup your files and your system. Most offer the option for automatic backups. Some allow you to schedule specific times, but look for those that will do automatic backups at startup and shut down, especially if your computer is on at irregular intervals. Many of these are transferrable from one operating system to another, but make sure you check. Some come with bootable discs, so you can fully restore your system, programs and files to a new hard drive if your original one died. But still consider utilizing cloud storage as an additional backup, especially since many offer some free storage space.

Finally, remember to *CHECK YOUR BACKUPS* to make sure that they are working properly.

(Continued from page 3)

Hoffmann. LaTex is a powerful document markup language for generating typeset documents. TeXstudio is an integrated environment for writing LaTeX documents with a goal to make writing LaTeX as easy and comfortable as possible. Therefore, TeXstudio has numerous features like syntax-highlighting, integrated viewer, reference checking and various assistants. TeXstudio runs on Windows, Unix/Linux, BSD and Mac OS X.

Screenshot link — Error Highlighting

http://a.fsdn.com/con/app/proj/texstudio/screenshots/errorHighlighting.png

youtube-dl – v2013.08.23.
http://rg3.github.io/youtube-dl/
Free Public Domain Python script by Ricardo Garcia Gonzalez et al. youtube-dl is a small command-line program to download videos from YouTube.com and a few more sites. It requires the Python interpreter (2.6, 2.7, or 3.3+), and it is not platform specific. It should work in your Unix box, in Windows or in Mac OS X.

Kernel Source – v3.10.9.
http://www.kernel.org/
Free GNU General Public License source code for all platforms by the Linux community.

Don't Forget! Be Safe Online!

October is National Cyber Security Awareness Month

See http://www.staysafeonline.org/

http://www.staysafeonline.org/ncsam/

PATACS Information

PATACS, Inc. 201 S. Kensington St. Arlington VA 22204-1141

Club Information call: 703-370-7649   **Web Site: www.patacs.org**

President	Jim Rhodes	703-931-7854	president(at)patacs.org
1st VP, Newsletter Exchange	Ron Schmidt	301-577-7899	director11(at)patacs.org
2nd VP, Membership Chair	Mel Mikosinski	703-978-9158	director4(at)patacs.org
Treasurer, Registered Agent, Internet Services	Paul Howard	703-860-9246	director2(at)patacs.org
Secretary, Meeting Setup	Bill Walsh	703-241-8141	director14(at)patacs.org
Director, APCUG Liaison	Gabe Goldberg		director10(at)patacs.org
Director, Vendor Liaison	(vacant)	volunteer needed	director12(at)patacs.org
Director, Linux Support	Geof Goodrum	703-370-7649	director1(at)patacs.org
Directors	Jorn Dakin, Sy Fishbein, Walter Fraser, Roger Fujii, Mel Goldfarb, Bob Rott, Nick Wenri		
Windows Support	Jim Brueggeman	703-450-1384	windows(at)patacs.org
Newsletter Editors	Blair Jones, Geof Goodrum		editor(at)patacs.org
Columnist	Lorrin Garson		newslettercolumnist(at)patacs.org

Posts is an official publication of the Potomac Area Technology and Computer Society (PATACS), a Virginia membership corporation. PATACS is a tax exempt organization under section 501(c)(3) of the Internal Revenue Code. Contributions are gratefully received and tax deductible.

Posts provides news, commentary and product information to PATACS members. Products or brand names mentioned may be trademeakes or registered trademarks of their respective owners. The contents of articles herein are the responsibility of the authors and do not necessarily represent PATACS, the Board of Directors, nor its members.

E-mail article submissions and reprint requests to editor(at)patacs.org

Membership Policy

Membership dues are $25.00 (U.S.Funds) per year, with a $15 surcharge for international mail. Membership in PATACS includes membership in all SIGs, access to the software libraries, and subscription to the Posts published 12 times per year in print by US Mail and PDF download by Internet. Applications may be obtained at any club meeting, by downloading from the website, by calling one of the officers or board members, or by writing to the club. A sample newsletter, membership application and related information may be obtained by enclosing $2 (for US addresses only) and mailing your request to the membership address. Please do not send cash by mail. Payment and applications may also be submitted at any meeting, or mail to: PATACS Membership, 4628 Valerie CT, Annandale VA 22003-3940

Advertisement Policy

Members' advertisements: Ads are accepted from members for non-commercial purposes at no charge. Copy should be sent to the Editor in the same format as article submissions. Commercial Advertisements: Ads are accepted from commercial advertisers at the rate of $40 per full page, per appearance, with discounts for multiple insertions. Smaller ads are priced accordingly. Payment for ads must be made in advance of appearance. Advertisers must supply a permanent address and telephone number to the editor.

Reprint Policy

Permission to reprint articles from the PATACS Posts is given to school, personal computer club, and nonprofit organization publications, provided that: (a) PATACS Inc. receives a copy of the publication; (b) credit is given to the PATACS Posts as the source; (c) the original author is given full credit; and (d) the article author has not expressly copyrighted the article. Recognition is one means of compensating our valued contributors

If you are moving

Please send your change of address to the club address as soon as possible to avoid missing issues.

Thank You!

Upcoming Meetings

Annual Meeting and Election of Directors

Wednesday October 2, 2013, 7pm at Carlin Hall

Ballots for the election of Directors will be distributed by email.

Microcenter Clinics

See http://microcenter.com/site/stores/instore-clinics.aspx for the latest news on these free clinics.

PATACS Meeting Information

Call (703) 370-7649 for meeting announcements or visit our web site at

http://www.patacs.org

Free Admission — Bring a Friend!

Arlington Meetings

Carlin Hall Community Center
5711 S. 4th Street, Arlington, VA 22204
http://www.patacs.org/arlingtonmeetings.html

General Meeting
1st Wednesday (10/2) 7pm

Technology and PC Help Desk (SIG)
4th Wednesday (10/23) 7pm

Board of Directors
3rd Monday (10/21) 7pm

Fairfax Meetings (with OLLI PC User Group)

Osher Lifelong Learning Institute (OLLI)
4210 Roberts Road, Fairfax VA 22032
http://www.patacs.org/fairfaxmeetings.html

General Meeting
3rd Saturday (10/19) 12:30pm

Online-Only Webinar
2nd Wednesday (10/9) 7-9pm
http://www.patacs.org/webinarpat.html