PATACS Posts

Newsletter of the Potomac Area Technology and Computer Society

October 2012 www.patacs.org

Useful Bits & Pieces #9 September 2012

By Lorrin R. Garson, PATACS

Windows 8 Released to Manufacturers

Microsoft has finished with the development and testing of Windows 8 and has released the operating system to computer manufacturers such as Dell, Asus, Acer, Hewlett-Packard, etc., so that they can start the process of installing Windows 8 on their computers for sale when the OS is launched in October 26th.

Hello Outlook.com, Adios Hotmail

If you are a user of Hotmail, you may want to look into the new Outlook.com that will eventually replace Hotmail. Outlook.com will have the look and feel of Windows 8 and is optimized for touchscreen devices. For a video from Microsoft and a link to download the new e-mail software, see http://windows.microsoft.com/en-us/windows/outlook/hom. For reviews see http://www.firstpost.com/tech/review-what-microsoft-has-got-right-with-outlook-com-400851.htm and http://reviews.cnet.com/e-mail/microsoft-outlook-com-e/4505-3536_7-35404526.htm.

Windows 8 and Backup

It seems that Microsoft will offer a new backup tool with Windows 8 (see http://blogs.msdn.com/b/b8/archive/2012/07/10/protecting-user-files-with-file-history.asp). A new utility called *File History* will provide continuous backup for Libraries, Desktop, Favorites and Contacts folders to an external storage device, but not to "the cloud". *File History* will not provide full system backup, although presumably users will still be able to use the Windows Backup tool to do this. ZDNet quotes Microsoft "…less than five percent of consumer PCs use Windows backup…", hence the development of *File History* to encourage people to take backup seriously.

Wiktionary

Everyone uses a dictionary from time to time. But groping for that thick book and flipping through the pages is so 19th century. Try Wiktionary at http://www.wiktionary.org. It's not the *Oxford English Dictionary* but it's easy to use and adequate for many if not most purposes.

(Continued on page 14)

Linux and Open Source News .... page 2
Free Virus & Malware Removal Tools from Kaspersky .... page 4
Buying A New Computer — Things To Think About (Part 2) .... page 6
Cyber Security Tip — Use Caution with USB Drives .... page 8
Building a Better System and Data Backup Strategy .... page 9
Are You Being Followed? .... page 10
Make Hard to Break Easy to Remember Passwords .... page 13
Evernote 4 .... page 13
Annual Meeting and Election Notice........page 15

Linux and Open Source News

By Geof Goodrum, PATACS linux(at)patacs.org

LXDE

By Cal Esneault, President of the Cajun Clickers Computer Club, LA and leader of many Open Source Workshops & SIGs

November 2011 issue, Cajun Clickers Computer News
http://cccclinuxsig.pbwiki.com www.clickers.org
ccnewsletter (at) cox.net

The Linux OS (Operating System) permits users to select from many front-end desktop environments (the interface software that controls mouse, touch screen, icons, etc.). Popular interfaces such as GNOME and KDE are powerful but can require high system resources. LXDE (Lightweight X11 Desktop Environment) is a simpler approach more suitable for netbooks, mobile devices, or older PC's. It is designed to be faster, more energy efficient, and be a better fit for the future of "cloud" computing. Since LXDE open-source software is based on X-windows, the commonly used system and network protocol that provides the basis for graphical user interfaces (GUI's), it can be used with all the popular Linux and BSD distributions (distro's) – Ubuntu, Fedora, OpenSUSE, Debian, etc.

LXDE originated as PCMan in 2006 by Hong Jen Yee with the file manager PCManFM as the first component.

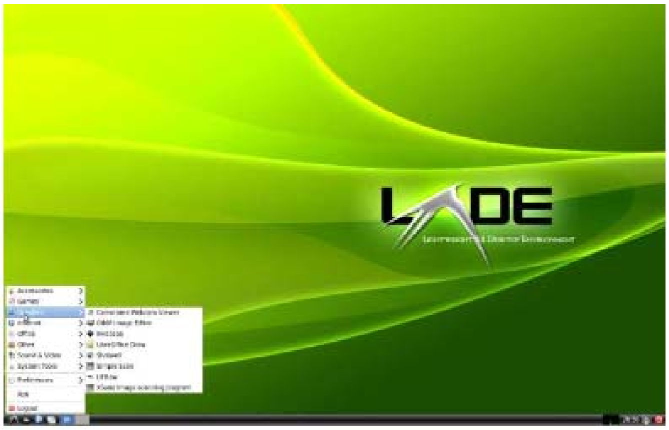
This community backed distro with OpenBox as the window mananger has risen rapidly in popularity. In May 2011, Lubuntu (the Ubuntu derivative using LXDE) was made an official Canonical distro and has surpassed the KDE-based Kubuntu in active downloads. On my system which has Ubuntu 11.04 as the main OS, I downloaded the LXDE desktop (see screenshot below).

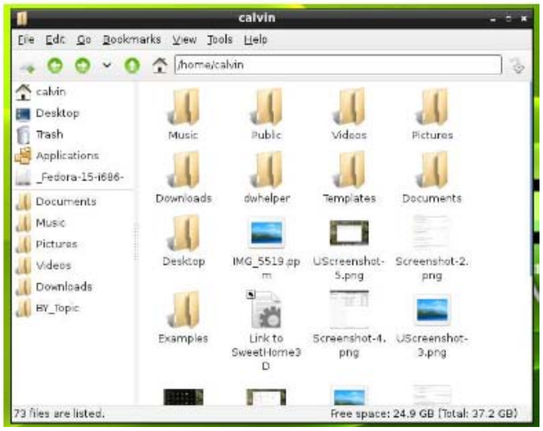
Note the traditional tree-and-branch menu system arising from the bottom panel. This reminds me of the older KDE 3.x family. There are no extra "widgets" or desktop panels now common in current KDE 4.x releases. Also, there are no side panels of "tiles" and pop-out icons present in the newer Unity or Gnome 3.x desktops. LXDE has a simple, clean interface which should be comfortable for traditional users, such as those familiar with Windows XP.

Below is a screenshot on my system using the PCManFM file manager:

Since I also have Gnome 3.x and KDE 4.X programs on my system, I have access to all of them through LXDE. If you want to have a less sophisticated system that runs on older equipment with minimum software overhead, do a fresh install of a dedicated LXDE distro.

For example, a Pentium II processor with 256 MB of RAM that was used for Windows 98 could work, or a later 600 MHz Pentium III with 512 MB of RAM should run well. Several major distro's provide a wide choice for your selection. For instance, the software provided by Lubuntu includes (among many others):





73 files are listed.
Free space: 24.9 GB (Total: 37.2 GB)

- GPicView (photo viewer)
- Leafpad (text editor)
- LXTerminal (command line access)
- OpenBox (window manager)
- PCManFM (file manager)

Most distro's also have versions to work with their latest versions. For example, Lubuntu 11.10 will be offered as one of the versions to be released this October. Check all this out at the LXDE.org website.

Featured Linux Software of the Month October 2012

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.

Evolvotron – v0.6.2
http://www.bottlenose.demon.co.uk/share/evolvotron/index.htm
Free GNU General Public License source code and executable packages for Debian, Ubuntu, Mandriva, and OpenSuSE by Tim Day. Evolvotron is an interactive "generative art" application to evolve images/textures/patterns through an iterative process of random mutation and user-selection driven evolution. If you like lava lamps, and never got tired of the Mandelbrot set, this could be the software for you. It's implemented using Qt, and is multithreaded.

fwbuilder – v5.1.0.3599 http://www.fwbuilder.org
Free GNU General Public License source code and executable packages for Debian/Ubuntu, Fedora/OpenSUSE/Red Hat by Vadim Kurland and Mike Horn. Firewall Builder consists of a GUI and set of policy compilers for various firewall platforms. It helps users maintain a database of objects and allows policy editing using simple drag-and-drop operations. The GUI and policy compilers are completely independent, which provides for a consistent abstract model and the same GUI for different firewall platforms. It currently supports iptables, ipfilter, ipfw, OpenBSD pf, Cisco PIX and FWSM, and Cisco routers access lists.

Letter Meister – v0.7b
http://www.lettermeister.javamex.com
Free licensed Java executable by Neil Coffey. LetterMeister is a word puzzle game. Using colored clues, rearrange the letters on the board to reconstruct an interlocking crossword grid. Choose your moves carefully to maximize your use of bonus squares and discover the identity of hidden letters. English, French, and Spanish vocabularies are included. Requires a Java runtime environment.

Kernel Source – v3.5.2.
http://www.kernel.org.
Free GNU General Public License source code for all platforms by the Linux community.

———————————————————————-

Screenshot links for the software listed

Evolvotron

http://www.bottlenose.demon.co.uk/share/evolvotron/gallery.htm

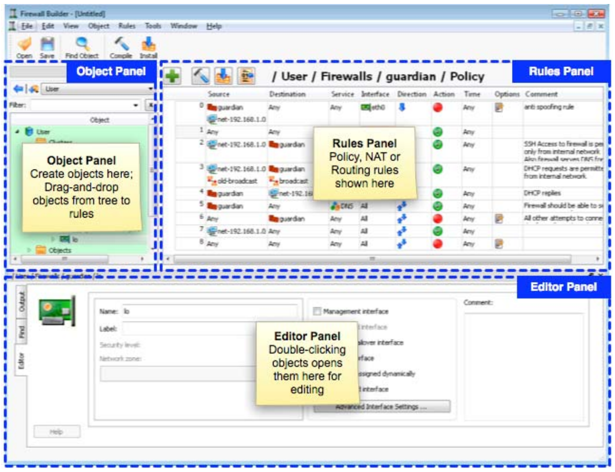
Firewall Builder

http://www.fwbuilder.org/4.0/images/fwbuilder_gui_layout.png

Letter Meister

http://i1-games.softpedia-static.com/screenshots/LetterMeister_2.jpg

———————————————————————-


Firewall Builder - [Untitled]
File Edit View Object Rules Tools Window Help
Open Save Find Object Compile Install
Object Panel
/ User / Firewalls / guardian / Policy
Rules Panel
Source Destination Service Interface Direction Action Time Options Comment
Rules Panel
Policy, NAT or Routing rules shown here
Object Panel
Create objects here; Drag-and-drop objects from tree to rules
Editor Panel
Name: lo
Label:
Management interface
Comment:
Editor Panel
Double-clicking objects opens them here for editing
Advanced Interface Settings ...
Help

Free Virus and Malware Removal Tools from Kaspersky

by Ira Wilsker, iwilsker@sbcglobal.net

Websites

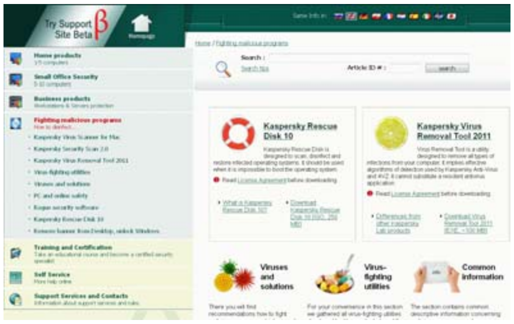
https://support.kaspersky.com/viruses
http://www.kaspersky.com/downloads/free-antivirus-tools
https://support.kaspersky.com/viruses/utility
https://support.kaspersky.com/viruses/avptool2011
https://support.kaspersky.com/viruses/rogue
https://support.kaspersky.com/viruses/rescuedisk
http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
https://support.kaspersky.com/viruses/deblocker
http://support.kaspersky.com/faq/?qid=208285998

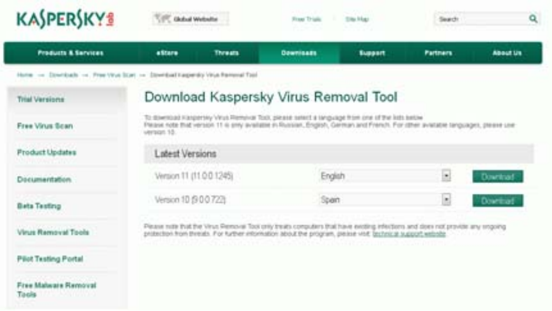
Many Americans may not be aware of the feisty Russian based computer security company Kaspersky, but it is the fourth largest overall security vendor in the world, the third largest vendor of consumer security software, and the fifth largest vendor of enterprise endpoint protection (source: Wikipedia). Headquartered in Moscow since its inception in 1987, Kaspersky currently has 29 regional offices around the globe, including U.S. offices in Boston and Miami. Kaspersky services over 300 million individual clients, and over 200,000 corporate clients, and provides its Kaspersky Anti-Virus engine and related software security services under license to over 120 other security vendors including Check Point, Juniper Networks, F-Secure, and many other software companies. According to Wikipedia, "In the United States, Kaspersky Lab was ranked as the fastest growing internet security software, based on NPD sales data." Kaspersky publishes a complete stable of security software for home, commercial, and mobile markets, and is typically among the highest rated security products in published reviews.

In addition to commercial products, Kaspersky also offers a comprehensive collection of free utilities to detect and remove viruses and other malware, including ransomware, and rogue software, from infected computers. These free utilities are only intended to clean infected computers, and not intended as full time protective software; Kaspersky (and others) happily sell security software for that purpose.

A summary of Kaspersky's free detection and cleaning services is online at support.kaspersky.com/viruses, and includes information and links for its many detection and removal utilities. Kaspersky offers a broad selection of these utilities, including a large (130 mb) and comprehensive virus detection utility Kaspersky Virus Removal Tool 2011 (support.kaspersky.com/viruses/avptool2011). According to the website, "Kaspersky Virus Removal Tool is a utility designed to remove all types of infections from your computer." The "2011" date may be misleading, as this product is continuously updated, and ready to run when downloaded. Kaspersky explains this as, "Kaspersky Virus Removal Tool 2011 provides no update function. The up-to-date version of the application with the latest version of anti-virus databases is always available on the website …" While the Virus Removal Tool 2011 is complete and up to date when downloaded, additional functionality is available during the scan process if there is current internet access, allowing for " ... non-signature search of malware based on "cloud" technologies." The detection and removal process is automated, and little or no user intervention is required while the scanner is running. This utility is one that I download fresh to a flash drive (along with several other utilities) if I know that I am going to clean an infected computer.

Some computers have been so severely infected that they cannot be booted, or have viruses and other malware that prevents traditional detection and removal utilities from executing. Kaspersky offers a free solution to this predicament with its Kaspersky





Download Kaspersky Virus Removal Tool

Latest Versions

Version 11 (11.0.0.1245)	English	Download
Version 10 (9.0.0.722)	Spain	Download

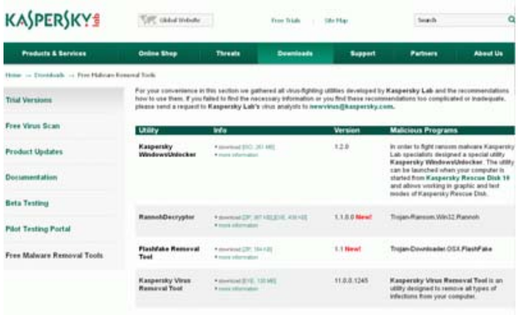
Rescue Disk 10 (support.kaspersky.com/viruses/rescuedisk). The website explains why it is necessary to use the bootable Rescue Disk 10 when system based utilities are unable to clean the infected computer, “Kaspersky Rescue Disk is designed to scan, disinfect and restore infected operating systems. It should be used when it is impossible to boot the operating system. In this case, disinfection is more efficient because malware programs do not gain control when the operating system is being loaded. In the emergency repair mode, you can only start objects, scan tasks, update databases roll back updates and view statistics.” The RescueDisk 10 file is a 236 mb ISO file that must be burned to a CD using any one of the many available ISO burners, which will make the CD bootable; simply copying or burning the downloaded ISO file to a CD will not create a bootable CD. Instructions on how to create a bootable CD using the ISO file are available on the website, and are also included with almost all ISO burning utilities. Most major CD burning utilities support the creation of bootable CDs using an ISO file; just be sure to check the ISO selection from the CD utility software menu. Once booted with the created Rescue Disk, the computer can be scanned using the included Kaspersky scanning engine which will effectively detect and kill most malware in circulation. After the computer is cleaned with Rescue Disk 10, the CD is removed, and the newly disinfected computer rebooted as normal. As is common after most contemporary infections, it may be necessary to reinstall any security software that was on the computer prior to the infection (maybe not a good idea, because it had already been proven to be vulnerable), or install a new security suite.

In a recent column I wrote about the nasty form of malware referred to as “ransomware” where an infected computer is locked by the malware, and supposedly not released until ransom is paid via a third party payment service to a cyber crook. This ransomware is often accompanied by a screen falsely announcing that child pornography or pirated software was found on the computer, threatening jail time and hefty fines if the ransom or fine is not promptly paid. The screen of the locked computer gives explicit instructions on how to pay the fine (ransom) to unlock the computer. Even if the fine/ransom is promptly paid, the computer will likely not be unlocked by the scammer. In addition to the ransom requested, the cyber crook also often loads other malware to the infected computer, including varieties of spyware and key loggers to steal valuable personal information, banking, shopping, and credit card information in order to perpetrate identity theft and other financial crimes.

Kaspersky offers an interactive free utility to explicitly unlock the purloined computer, and allow the removal of the ransomware. Kaspersky WindowsUnlocker is a large (236 mb) ISO file that can be burned to a CD or installed to a bootable USB flash drive; detailed instructions on how to create the CD or bootable flash drive are available from Kaspersky at support.kaspersky.com/faq/?qid=208285998.

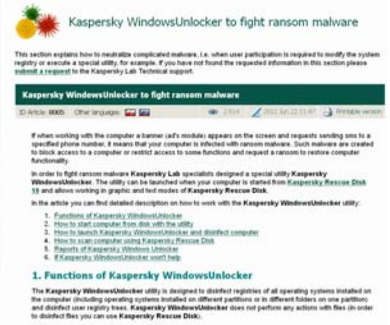
The bootable media also includes an updated copy of Kaspersky’s Rescue Disk utility, which will be used in conjunction with the WindowsUnlocker. Once the bootable media is created, the computer is booted with it, following the instructions provided (above) by Kaspersky. The WindowsUnlocker utility will scan the registry and remove any traces of the ransomware from the registry (these hidden registry entries are often referred to as a form of “rootkit”), and then run the malware detection and removal software to complete the cleaning process. This process will likely remove the rasnsomware as well as any additional malware that it may have installed or any malware that had previously infected the computer. The bootable media is removed from the computer and then the computer is rebooted normally; if successful, the ransomware should be gone. It will then be nec-

(Continued on page 7)



For your convenience in this section we gathered all virus-fighting utilities developed by Kaspersky Lab and the recommendations how to use them. If you failed to find the necessary information or you find these recommendations too complicated or inadequate, please send a request to Kaspersky Lab's virus analysts to newvirus@kaspersky.com.

Utility	Info	Version	Malicious Programs
Kaspersky WindowsUnlocker	• download [ISO, 261 MB] • more information	1.2.0	In order to fight ransom malware Kaspersky Lab specialists designed a special utility Kaspersky WindowsUnlocker. The utility can be launched when your computer is started from Kaspersky Rescue Disk 10 and allows working in graphic and text modes of Kaspersky Rescue Disk.
RannohDecryptor	• download [ZIP, 307 KB][EXE, 436 KB] • more information	1.1.0.0 New!	Trojan-Ransom.Win32.Rannoh
Flashfake Removal Tool	• download [ZIP, 184 KB] • more information	1.1 New!	Trojan-Downloader.OSX.FlashFake
Kaspersky Virus Removal Tool	• download [EXE, 130 MB] • more information	11.0.0.1245	Kaspersky Virus Removal Tool is an utility designed to remove all types of infections from your computer.



Kaspersky WindowsUnlocker to fight ransom malware

This section explains how to neutralize complicated malware, i.e. when user participation is required to modify the system registry or execute a special utility, for example. If you have not found the requested information in this section please submit a request to the Kaspersky Lab Technical support.

Kaspersky WindowsUnlocker to fight ransom malware

ID Article: 8005 Other languages: 2314 2012 Jun 22 11:47 Printable version

If when working with the computer a banner (ad's module) appears on the screen and requests sending sms to a specified phone number, it means that your computer is infected with ransom malware. Such malware are created to block access to a computer or restrict access to some functions and request a ransom to restore computer functionality.

In order to fight ransom malware Kaspersky Lab specialists designed a special utility Kaspersky WindowsUnlocker. The utility can be launched when your computer is started from Kaspersky Rescue Disk 10 and allows working in graphic and text modes of Kaspersky Rescue Disk.

In the article you can find detailed description on how to work with the Kaspersky WindowsUnlocker utility:

1. Functions of Kaspersky WindowsUnlocker
2. How to start computer from disk with the utility
3. How to launch Kaspersky WindowsUnlocker and disinfect computer
4. How to scan computer using Kaspersky Rescue Disk
5. Reports of Kaspersky Windows Unlocker
6. If Kaspersky WindowsUnlocker won't help

1. Functions of Kaspersky WindowsUnlocker

The Kaspersky WindowsUnlocker utility is designed to disinfect registries of all operating systems installed on the computer (including operating systems installed on different partitions or in different folders on one partition) and disinfect user registry trees. Kaspersky WindowsUnlocker does not perform any actions with files (in order to disinfect files you can use Kaspersky Rescue Disk).

Buying A New Computer –Things To Think About (Part 2 Of 3)

By Phil Sorrentino, Past President, Sarasota PCUG, Florida
February 2012 issue, Sarasota PCUG Monitor www.spcug.org pcugedit@verizon.net

Last month we discussed manufacturers, laptop vs. desktop, and looked at the CPU. Now it's time to think about a few more things.

Let's look at a laptop first because there aren't as many considerations. Because of a laptop's physical size and configuration, there are only a few things that can vary and therefore make you make a decision. The first one is Display size. Today, display sizes seem to be between about 14 and 18 inches. Larger displays can give you more webpage space, but will probably lead to heavier laptop, a consideration if you are going to carry it around a lot.

Another parameter you may find advertised with a laptop is Battery Life. This becomes important if you are going to use the laptop without ac power for long periods of time, like on a flight from New York to Florida. (For really long flights, you might want to have a second battery.) Today's typical Lithium-Ion batteries will provide from around 3 to around 6½ hours of use time. To get the longer use time, the battery will probably be larger and therefore heavier, again a consideration only if you intend to carry it around a lot.

All computers, laptops included, rely on two types of memory, volatile storage, called RAM (Random Access Memory), and Non-volatile storage, typically a Hard Disk Drive (HDD). The sizes of both of these are decision to be made. We haven't discussed the Software Operating System (OS) yet, but today the OS will probably be Windows 7, Home Premium. So for a Windows 7 computer, it is suggested that a minimum of 2 GB of RAM be included. (If the CPU is a 32-bit CPU then the maximum would be 4 GB. If the CPU is a 64-bit CPU then today the maximum is 16 GB, for Windows 7 Home Premium and 192 GB for Windows Enterprise, Professional, and Ultimate, but the particular laptop hardware will probably limit the RAM to something less.) Note that increased memory does not yield any substantial increase in weight, so get as much as you can.

Now for the Hard Disk Drive. Most, if not all, laptops have only one HDD, although it can be partitioned into many logical drives, e.g. C:, D:, etc. For a Windows 7 computer, it is suggested that the HDD size be at least 200 GB. The OS and applications could take as much as 100 GB, leaving only 100 GB for data (documents, pictures, videos, music). Today, most machines will have between 400 and 1,000 GB of HDD space. Note that increased HDD size does not yield any substantial increase in weight, again, so get as much as you can.

Sooner, than later, all laptops are called upon to access the Internet. This can be accomplished by a wired connection to an Internet Service Provider (ISP), or a wireless connection to the ISP. All of today's laptops provide both of these connection capabilities. The wired connection is provided by an RJ-45 plug somewhere on the back or side of the laptop. The wireless connection is provided by 802.11 b, g, or n Local Area Network communications radio transmitter and receiver built into the laptop motherboard (the antenna is usually someplace in the laptop cover).

802.11 wireless communications is available in many public places like airports, some shopping centers, and libraries, and is referred to as Wi-Fi, which stands for Wireless Fidelity. This type of wireless communications uses the 2.4 GHz band for communicating with a wireless access point, which is typically part of a router. The router in turn connects to the ISP, through a modem. The b, g, or n specifies the particular signaling technique and communications protocols to be used. 802.11n is the newest and the most capable, having the fastest transfer rate (200 to 300 Mbps). 802.11g is the most ubiquitous, and is backwards compatible with the older 802.11b. n is backwards compatible with both g and b. Today all laptops are at least g compatible and many newer laptops are n compatible. The wireless communications capabilities are probably not a decision factor, unless you specifically want the newest 802.11n capability.

Laptops typically have an optical CD/DVD Drive which is capable of reading and writing CDs and DVDs. Some of the newer, and more expensive laptops, are including a Blue-ray Drive which is capable of reading and writing Blue-ray Disks (BD). These BD drives are backwards compatible with DVDs and CDs so they can read and write all three types of optical storage disks. (Just a quick review of capacities - CDs hold 700 MB, DVDs hold 4.7 GB, and BDs hold about 25 GB.) The optical drive is only a decision point if you are specifically interested in reading and/or writing BD disks, otherwise there is little difference between manufacturers optical drive products.

Most of the newer laptops have a camera, typically just above the display in the center. The camera faces the user so it can be used for audio/video telecommunications such as Skype and Google Talk. This is definitely a decision point if you intend to use the video calling capabilities. A camera usually does not add much to the price and may prove to be a useful capability in the future.

All laptops have audio capabilities, usually a microphone input, provided by a 1/8th inch mono mini-jack, and a stereo output provided by a 1/8th inch stereo mini-jack. The microphone input can be used for audio/video telecommunications like Skype and Google Talk. The stereo audio output can also be used to drive a set of good external speakers or even the audio of some older televisions. Audio capabilities are not a decision point.

All laptops have an external Monitor output. On older laptops the output connector is a 15 pin VGA female connector. On newer laptops the video output is available on an HDMI (High Definition Multimedia Interface) connector along with audio. HDMI is the best way to connect your laptop to a newer television.

All laptops have USB 2.0 interface ports. The number of ports may be a decision point. And the newer USB 3.0 may show up on some newer, more expensive laptops. Some laptops (not many) may have other types of interface ports such as Firewire or eSATA. This is definitely a decision point if these types of interfaces are needed.

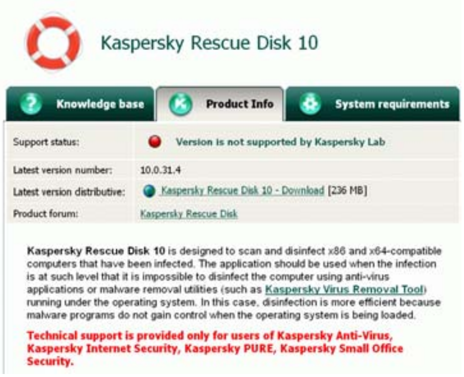
So far we've looked at all the important things for the purchase of a laptop. Next month we'll cover Desktops and some other miscellaneous things to consider.

(Continued from page 5)

essary to install (or reinstall) a comprehensive security suite, and any previously installed security software may have been compromised by the ransomware (malware).

In addition to the broad spectrum scanners already mentioned, Kaspersky offers an extensive collection of small, free scanners for specific scanning tasks, and removal of difficult infections. Several of these specific removal utilities are intended to detect and neutralize individual ransomware, illicit file encryption malware, rootkits, and other threats. The comprehensive list of free security scanners available for download is located at kaspersky.com/downloads/free-antivirus-tools.

Hopefully, you will never need to utilize these excellent, free malware detection and removal utilities from Kaspersky, but a familiarity with them may provide some degree of "peace of mind" in this dangerous and threatening cyber world. It is nice to know that they are available if (when) you ever need them.

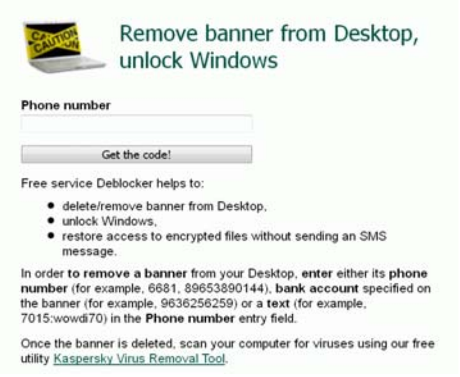


Kaspersky Rescue Disk 10

Support status:	● Version is not supported by Kaspersky Lab
Latest version number:	10.0.31.4
Latest version distributive:	Kaspersky Rescue Disk 10 - Download [236 MB]
Product forum:	Kaspersky Rescue Disk

Kaspersky Rescue Disk 10 is designed to scan and disinfect x86 and x64-compatible computers that have been infected. The application should be used when the infection is at such level that it is impossible to disinfect the computer using anti-virus applications or malware removal utilities (such as Kaspersky Virus Removal Tool) running under the operating system. In this case, disinfection is more efficient because malware programs do not gain control when the operating system is being loaded.

Technical support is provided only for users of Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky PURE, Kaspersky Small Office Security.



Remove banner from Desktop, unlock Windows

Phone number

Free service Deblocker helps to:

- delete/remove banner from Desktop,
- unlock Windows,
- restore access to encrypted files without sending an SMS message.

In order **to remove a banner** from your Desktop, **enter** either its **phone number** (for example, 6681, 89653890144), **bank account** specified on the banner (for example, 9636256259) or a **text** (for example, 7015:wowdi70) in the **Phone number** entry field.

Once the banner is deleted, scan your computer for viruses using our free utility Kaspersky Virus Removal Tool.

Cyber Security Tip ST08-001 – Using Caution with USB Drives

By Mindi McDowell

Produced 2008, 2011 by US-CERT, a government organization http://www.us-cert.gov/cas/tips

Note: This tip was previously published and is being re-distributed to increase awareness.

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive.

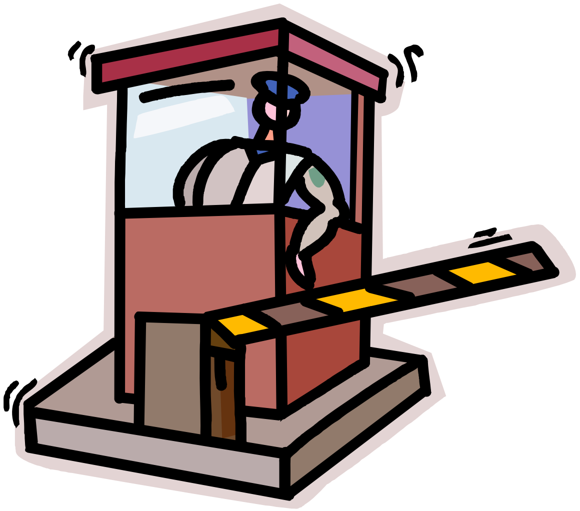
Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see Protecting Portable Devices: Physical Security for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data? There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Take advantage of security features – Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see Protecting Portable Devices: Data Security for more information).
- Keep personal and business USB drives separate – Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

- Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see Understanding Firewalls, Understanding Anti-Virus Software, and Recognizing and Avoiding Spyware for more information). Also, keep the software on your computer up to date by applying any necessary patches (see Understanding Patches for more information).
- Do not plug an unknown USB drive into your computer – If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.
- Disable Autorun – The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows, Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."



Building a Better System and Data Backup Strategy

By Gabe Goldberg, APCUG Advisor, Region 2
destination.z@gabegold.com

Obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

Because operating without reliable backup risks corporate health and can be a profoundly career-limiting move, the most fundamental resolution for mainframe professionals is "backup, backup, backup." But beyond that, some may ask where to start and what to do? Challenges and opportunities to better preserve critical software and data resources divide—though not precisely—between technology and human issues.

Let's address backup—and its indispensable partner, restore—which are separate from more complex issues of business continuity (BC), formerly called disaster planning/recovery. While critical for BC, backup/restore are hardly a complete solution for it. Consider these tips and best practices:

Technology/Logistics Tasks

1) **Remember why you're doing this.** Let business reasons for backup govern your decisions. Consider disaster recovery, user errors, audit/disclosure/preservation requirements.
2) **Back up everything that matters.** Do you know where your data is? It's no longer just nicely boxed in server rooms. Besides servers, desktop and laptop computers, tablets and smartphones can contain essential nowhere-else data. If you'd miss it, back it up. Remember Hardware Management Console (HMC) data, and back it up regularly to a USB drive, DVD, via FTP, etc.
3) **Integrate backup processing and data as much as possible.** No matter why you're restoring data, it's messy and risky to have to use too many tools to recover varying format/location data.

(Continued on page 11)

Are You Being Followed?

By Linda Gonse, Editor/Webmaster, Orange County PCUG, California
December issue, nibbles & bits www.orcopug.org editor (at) orcopug.org

Obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

You may not even suspect you are being followed. But, as many as 60 ad networks may be tracking you on the web right now! What's more, they may be selling personally identifiable details about you.

If this disturbs you, you can put a stop to it. You can quickly opt out from advertising networks —each has multiple clients! — with just a few mouse clicks.

The National Advertising Initiative (NAI) is a cooperative of dozens of online ad networks that track you. An NAI statement says it developed an Opt-out Tool "in conjunction with our members for the express purpose of allowing consumers to 'opt out' of the behavioral advertising delivered by our member companies." To this end, NAI offers a YouTube video on their home page showing you how the Opt-out Tool works. (You can also see the enlarged video before you go to their site at http://bit.ly/ruQt9)

Basically, the Opt-out Tool, which will not be installed on your computer, examines cookies (small text files) on your computer and identifies those member companies that have placed an advertising cookie on it.

When a member company's cookie is identified by the Opt-out Tool, you simply check the box next to the company name. If you are strongly motivated (or highly frustrated), check the "Select All" box! Then, click the "Submit" button, and you're done. The cookies will be removed for the selected companies and your opt-out status will be automatically verified.

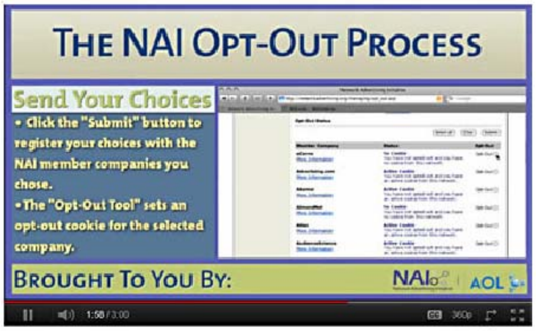
Go to the NAI website at http://bit.ly/sNMlj to get the opt-out process started.

There are two caveats. 1. Opting out of a network does not mean you will no longer see online advertising. But, the network from which you opted out will no longer be tracking you personally and displaying ads that are "tailored to your web preferences and usage patterns." Isn't that the idea? 2. Networks voluntarily allow opting out. It isn't a legal mandate. Also, technical glitches may occur. Cookies from any of these networks may reappear. So, use the Opt-out Tool regularly.

Quantcast Measurement and Advertising does not participate in the National Advertising initiative, but also offers you the ability to opt-out of their ads based on your interests.

Quantcast claims it doesn't store your IP address or any other personally identifiable information. "But, if you prefer not to receive interest-based content and advertisements enabled by Quantcast and not to have Quantcast measure your pattern of website visits or other online media consumption, you can opt-out by using our opt-out tool" at http://bit.ly/vNAXO.

Opting out is the only way you can avoid being tagged, tracked and tempted by advertisers who know your purchasing history. By opting out you can end hunting season by advertisers who are determined to bag your money.

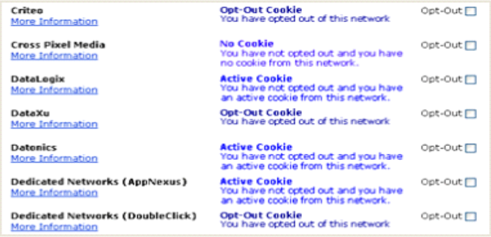


THE NAI OPT-OUT PROCESS

Send Your Choices

- Click the "Submit" button to register your choices with the NAI member companies you chose.
- The "Opt-Out Tool" sets an opt-out cookie for the selected company.

BROUGHT TO YOU BY:



Criteo More Information	**Opt-Out Cookie** You have opted out of this network	Opt-Out □
Cross Pixel Media More Information	**No Cookie** You have not opted out and you have no cookie from this network.	Opt-Out □
DataLogix More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.	Opt-Out □
DataXu More Information	**Opt-Out Cookie** You have opted out of this network	Opt-Out □
Datonics More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.	Opt-Out □
Dedicated Networks (AppNexus) More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.	Opt-Out □
Dedicated Networks (DoubleClick) More Information	**Opt-Out Cookie** You have opted out of this network	Opt-Out □

A few of the networks that may have placed one or more cookies on your computer.

(Continued from page 9)

4) **Ensure backups are complete.** Some utilities won't include expired files in full-volume backups, or won't write them to tape. After backup procedures are created, verify file inventories are complete.

5) **Plan ahead for restoring data in a recovery center.** Require vendors to provide emergency keys/codes/passwords for using their products away from home.

6) **Automate.** As much as possible, avoid manual steps in backing up data, documenting "what's where" for each backup and how to restore it.

7) **Create duplicate/redundant/separate backups.** Single backup volumes have huge capacity, so losing or damaging one can be a catastrophe. Data Facility Storage Management Subsystem's (DFSMS) duplex option simplifies this. Don't let one bad tape volume spoil a disaster-recovery drill—or a real disaster recovery.

8) **Be secure.** Maintain strict control of backup media to avoid a massive data breach appearing in the *other* media.

9) **Use offsite storage.** You won't win an award for stellar backup if all data copies are destroyed at once by fire, earthquake, hurricane, flood, or tornado. Use enterprise-worthy shipping, perhaps not local delivery services, and don't send duplicates together!

10) **Encrypt whatever leaves your local facility**. No matter how it's shipped or where it's sent, don't let "out of sight" mean "out of control."

11) **Remember stored backup media when changing IT technology.** Especially if you're subject to long-term retention (and retrieval) requirements, don't let older backup generations become unreadable. Include backup migration in equipment-upgrade planning.

12) **Automate failure notification.** Don't rely on manual detection and alerting; it's too easy for processing oddities to become routine without appropriate people knowing.

Human/Management Challenges

1) **Ensure BC.** Meaningful disaster planning/drill/ recovery requires using standard live backup files to recreate enough production operation to remain in business. To avoid unpleasant surprises, restore and verify "everything that matters" working properly.

2) **Understand varying backups**. Full, incremental and differential backups have different purposes, strengths and weaknesses, as do tape, DASD, virtual tape and FlashCopy technologies. Apply them appropriately to data with special requirements such as DB2 databases, which benefit from DS6800 FlashCopy consistency groups, creating consistent point-in-time copies across multiple volumes.

3) **Back up critical files especially carefully and often.** What would you do without VM's system directory, TSO's user attributes data set (UADS) , or a Resource Access Control Facility (RACF) database? Most directory management tools allow backing up directory files; it's useful and comforting to have a few copies, just in case. Always know which copy is authoritative and protect these files as critical, high-exposure data.

4) **Plan backup cycles to match business needs.** No backup plan or technology fits all situations. High volatility or transaction rates processing mission-critical or customer-sensitive data might need real-time offsite mirroring; ensure that it's far enough away to prevent both data centers being affected by the same incident. More leisurely environments handling fewer or more-easily reconstructed transactions might only require daily backups.

5) **Test backup/restore periodically.** Appearances can be deceiving; backups seeming to run normally might not be doing anything useful. Occasionally—but reliably—test all backup aspects by restoring and verifying data. This also ensures that restore processes aren't used for the first time in a crisis situation. Even if backups have worked flawlessly, that's not the time to learn how to restore data.

(Continued on page 12)

(Continued from page 11)

6) **Document everything.** This includes automatic and manual processes, tools used, file formats, data placements, error recovery, etc. Ensure information is current; don't let "small" changes creep in via oral tradition updates. Keep documentation duplicates onsite, at BC site, perhaps at operations or system programmers' homes, or on keychain USB drives. Write processes as non-technical, simple checklists that someone can handle cold when seeing them for the first time.

7) **Train operations and other staff on backup technologies and processes.** Ensure that everyone understands not just backup's critical nature but also how data is being protected, so they're not robotically following mysterious procedures.

8) **Train operators** to notice and notify on oddities as well as failure/warning alarms. It's too easy for minor glitches to be ignored and grow into major problems.

9) **Educate users and management in what's done and what's possible.** Help them be realistic in expectations and demands. Ensure they have a voice in designing and planning backup protections. Backup/restore/BC are *not* purely technical issues; they're fundamental corporate and line-of-business decisions.

10) **Provide user-initiated restore.** Within reasonable and announced constraints, allow users to automatically restore files without technical support. Of course, ensure that only original data owners can do this.

11) **Backup is not archive.** Be clear that backups are not forever and that arbitrarily old data cannot be restored. If desired, provide file archiving—user-driven or automated—separate from backup.

12) **Consider risks of human error or malicious behavior.** Online-only backup might be vulnerable to simultaneous destruction of original data and all copies. So, combining online/offline/offsite backups adds reliability, as does separation of duties requiring multiple people to perform sensitive tasks.

As mundane as managing backup is, no "Backup Professional" certification is available. It's a foundation of data center survival. It's best when never needed but potentially catastrophic when missing. Once established and verified, backup processing needn't be burdensome, as long as it's remembered and integrated into change management.

Gabe Goldberg has developed, worked with and written about technology for decades.

(Continued from page 13)

As I read an article, an email, a webpage, I just highlight the information that I want to save, right mouse click add to Evernote 4.0, and I have the article. It is clean and usually just the information that I want, usually eliminating ads or other information that is not part of the article. If any of it does get into the note, I can delete it. I can also add something that I missed or was on a different part of the screen. I can edit the formatting, and other typical text edits. I can even change the font or font size.

Evernote does include a link to the original document and links in the article are live. I always like to include a link to the original make sure that the author is cited and given proper credit.

Once I have created an Evernote, it will sync with all of my other devices that are signed into my account. So when I read an article on my desktop, I can create a note and it will almost immediately be available on my notebook, my iPad, my iPod, and my netbook. I can share the article with others via Twitter, Facebook, or email directly from Evernote.

The program is available for mobile devices with iOS, Android, Blackberry, Windows Phone 7 and WebOS as well as computers with Mac OS X, Windows, Safari , Chrome, and Firefox.

There are some limits to the program which can be addressed with a premium account for $45 a year or $5 a month. Evernote can be downloaded from http://www.evernote.co and for info comparing the free account verses the premium account, see http://www.reviewsync.com/evernote-pricing.htm . The iOS & Android versions can be found in their respective Apps Store.

Make Hard To Break, Yet Easy To Remember Passwords

By Doris Collins, Member, ccOKC (Computer Club of Oklahoma City)
May 2012 Issue, eMonitor www.ccokc.org
DJCollins1122 (at) aol.com

We all know that simple passwords are dangerous. If you're using any of the following for passwords (or forms thereof), you probably aren't as secure as you think:

- Names of Pets
- Birth date
- Last 4 digits of your SS#
- Kid's Names
- Grandkid's Names
- Parent's Names
- Addresses
- Phone Numbers
- The word Password

Did I Catch You? Well, It Gets Even Worse!

Even if you're not using any of the above, but are still using simple words (like car, bike, etc.) for your passwords, you're accounts are still pretty easy to break into. Now, a better password looks more like this:

```
      ks86jw03ts92ctb02
```

Although some would argue that it's not better than what most people have been using thus far. Yeah, yeah, I know what you're thinking, "How the heck am I supposed to remember that thing? It's 17 random letters and numbers!" Read on. That password is as easy to remember as any other - if you understand how it was constructed:

It's based on a fictitious Smith family with a daughter named Kelly and a son named Tyler. They have a 2003 Jeep Wrangler and an 02 Chevy Trail Blazer. Now, let's take those facts and look at the password again:

- ks — Kelly Smith, born in 1986
- jw03 — Jeep Wrangler, 2003 model
- ts92 — Tyler Smith, born in1992
- ctb02 — You guessed it, Chevy Trail Blazer
- 2002 model year

I simply took the first initials of everyone and everything involved, then the year they were born (or built). It's a lot tougher to guess a password like that, but still very easy to remember.

Evernote 4

Review by Hewie Poplock, APCUG Director; VP, Central Florida Computer Society
Hewie's Views & Reviews
http://www.hewie.net

I like to share information, especially with members of my user group. I read a lot of articles about computer hardware & software. When I find an article of interest, which may be news, pricing, reviews, or tutorials, I have to decide how to keep that information. I often save it as an Acrobat PDF file, or I may copy and paste the article and email to myself, or send the link to myself.

I frequently forget where I stored them, to follow through with a link, or to go back later to save it. Many times I do not even remember the article or how I tried to save it.

I have actually created an email address to send myself articles to keep track of them in one place. I have begun to save other articles in several folders in an attempt to become organized.

Recently I was asked about a free program that I tried a few years ago, Evernote. I decided to once again take a look at it and discovered that it is an organizational tool that I need to be using. Since I have started using it, I find it to be an important part of my everyday computer life.

(Continued on page 12)

(Continued from page 1)

Want to make it just a click away? Make a short cut on your desktop by

(a) right-clicking anywhere on the desktop, select “new” and then “shortcut”,

(b) put the URL in space indicated and left-click on “Next”, and

(c) enter the name of the shortcut (say Wiktionary) and left-click on “Finish”.

If you drag and drop that shortcut on to the taskbar (Windows 7), it will be pinned to your default browser (Firefox in my case) so that if you subsequently right-click on the browser’s icon in the taskbar, you can select this pinned object for quick access. Welcome to the 21st century.

Microsoft Download Center

Many (most?) have Microsoft Windows updates set to be downloaded and installed automatically on “patch Tuesday”, but what about such things as drivers, service packs, templates, clip art, security software, Microsoft Knowledge Base for help, Xbox and games, Skype, etc. Microsoft Download Center at http://www.microsoft.com/en-us/download/default.asp can be very informative and helpful.

October is Cyber Security Awareness Month
http://www.staysafeonline.org/ncsam/

Devicescape

Have you heard of Devicescape, “The WiFi Offload Company”? If not yet, you soon will. This company has developed software that it licenses to cell phone companies to be installed on cell phones used by their customers. The software takes advantage of unsecured WiFi sites to direct cell phone traffic from often over-loaded cellular networks to WiFi, which is generally faster and free for the taking. The software uses WiFi sites (reportedly 8 million in Devicescape’s database) at coffee shops, fast food restaurants, libraries, etc., but not residential sites. The software is sufficiently sophisticated to not select heavily loaded WiFi sites. Why would cell phone companies be interested in this technology? By taking advantage of open WiFi sites, traffic on their cellular circuits is reduced which also reduces investment needed to keep up with increasing amounts of data their customers download over cell phone circuits. See http://devicescape.com

Removing Security Software

Have you ever experienced difficulty uninstalling security software like antivirus or spybot removers, such as AVG, CA, McAfee, Symantec (Norton), Panda and Trend Micro? AppRemover to the rescue. This free software is designed to identify and uninstall security applications. See
http://download.cnet.com/AppRemover/3000-2096_4-10909880.htm
for a description and review. AppRemover can be downloaded and installed from
http://www.appremover.com.

Microcenter Clinics

For details on free clinics at local MicroCenter stores see
http://www.microcenter.com/instore_clinic/sign_up.html

PATACS Information

PATACS, Inc. 201 S. Kensington St. Arlington VA 22204-1141
Club Information call: 301-577-7899 **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	Neal Grotenstein		director12(at)patacs.org
Director, Newsletter Editor, Llinux 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 Brueggerman	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!

Annual Meeting

October 3rd, Walter Reed Community Center, Arlington, etc. 7 PM, Conference Room. Agenda: Election of Officers, club reports, member questions. Balloting for the election can be by email, sent to ballot@patacs.org, or in person at the annual meeting. E-mail ballots were sent in late August.

Slate of candidates for Officers — 2-year terms:

President James Rhodes
1st VP Ron Schmidt
2nd VP Mel Mikosinski
Treasurer Paul Howard
Secretary Bill Walsh
Vote for five officers, write-ins allowed on ballot.

Board Members-at-Large will be on next year's ballot.

Election commissioners are Mel Goldfarb and Jim Brueggeman, via email at the address noted above.

PATACS Meeting Information

Call 703-370-7649 for meeting announcements or visit web site at http://www.patacs.org/

Free Admission — Bring a Friend!

Arlington Meetings
(temporary location through January 2013 — please check website)

Walter Reed Community Center
2909 S. 16th St, Arlington VA 22203
http://www.patacs.org/arlingtonmeetings.html

General Meeting
1st Wednesday (10/3) 7pm
Annual Meeting and Election
see page 15 for more information

Internet Special Interest Group (SIG)
4th Wednesday (10/24) 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 (10/20) 12:30pm

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

Board of Directors
3rd Monday (10/15) 7pm

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

First Class

TEMP-RETURN SERVICE REQUESTED