

MONITOR

Vol. 31, No. 5

May 2013

Next Meeting
Tuesday, May 14

Extended Help's Half Hour

Contents

Improve Your Facebook Privacy and Security	Ira Wilsker	1
Still Holding on to XP or Windows 7?	Bob Rankin	3
Free Malware Removal Utilities from Kaspersky	Ira Wilsker	5
Who's Driving this Bus Anyway?	Dave Helmer	9
On the Shelves Now	Ira Wilsker	11
Holy Cow! Is this a Virus?	Linda Gonse	14
Review: The Artists Guide to GIMP	Bill Treadwell	16
Review: Kingston HyperX SSD	George Harding	17
Sources of Support for Linux Open Source Software		18
Giving Internet TV a Try	Gene Olson	21
Gizmo's Freeware		20
Society News		23
The Lighter Side		23



Improve Your Facebook Privacy and Security

by Ira Wilsker

However we personally feel about it, Facebook has become enormously popular. According to Facebook's Key Facts page (newsroom.fb.com/Key-Facts), Facebook has, "More than a billion monthly active users as of December 2012. ... 618 million daily active users on average in December 2012. 680 million monthly active users who used Facebook mobile products as of December 31, 2012." These numbers are impressive, indicating extreme growth in Facebook utilization, since its introduction in 2004. One issue facing Facebook, as well as many other social networking and online services, is the privacy and security of its users. Sadly, the small percentage of the

global population that wants to commit a variety of cybercrimes against innocent individuals have found that social networking services are a fertile hunting ground, and Facebook is no exception.

Facebook is well aware of the risks that its users face on a regular basis, and actively revises its system and policies in order to mitigate the risks to its billion users. While Facebook does what it can to secure its system, Facebook users must proactively choose the appropriate security settings offered by the service, engage in safe online practices, and have appropriate security software installed on their computers or other devices. Users must be cognizant of several facts when they post anything on a social network, such as Facebook; first, nothing posted online is totally private, and regardless of selected settings, it is always possible for others, including those with illicit intent, to access postings. On Facebook, anytime a user clicks on a “Like” button, some of their personal information is gathered by the “liked” page, and can be used for a variety of purposes as the users' data can be collected and catalogued. Also be totally aware that once something is posted online, it is effectively forever available, even after being deleted by the user. Facebook may become a virtual diary that may be accessed later by potential employers, social acquaintances, government agencies, and others for both totally legitimate purposes and dangerous dishonest use.

In the initial registration process of becoming a Facebook user, personal information including name, email address, and other information was provided to Facebook. People join Facebook primarily as a medium of communications, with the simple ability to locate other users and have them locate you on the Facebook network. Users need to determine who can find their personal information and contact them, and then set the Facebook privacy settings accordingly. Personal listings access may be restricted by the user by selecting one of the privacy settings that can allow everyone to locate the user, approved friends, or even a “friends of friends” that provides a geometrically larger universe of potential friends. While many users take pride in their huge number of friends on Facebook, often using the large number of friends as a form of status symbol, that also means that the same huge group of friends is more likely to include users who may pose privacy and security threats to the user.

Facebook users can easily access and modify security settings by opening the account control menu by clicking on the “gear” icon on the top right edge of the Facebook menu bar, and then selecting “Privacy Settings”. This opens the “Privacy Settings and Tools” which controls who can see your posts and look up your personal information. Once the “Privacy Settings and Tools” window is open, the left margin of that webpage offers additional security controls that the users should make use of. Under the “Timeline and Tagging Settings” the user can control who can post on their timeline, who can view the users' timeline, and can control the tagging and posting of images and posts.

Some Facebook users are unfortunately the victims of cyber stalking and cyber bullying; the “Blocking” menu icon on the left margin opens the “Manage Blocking” window. It is here that the user can create a “Restricted List” which controls who specifically can see information and posts. From this location unwanted users can be blocked by entering their name or email address, which means that the person blocked can no longer be your friend on Facebook or otherwise interact with you. Using a similar, simple procedure, the user can easily block app requests or event invites from other specific users or groups. Individual apps can be stopped from contacting you and accessing your non-public information on Facebook.

Facebook itself offers substantial privacy and security assistance and information

that users may use in order to improve their security and safety while on Facebook. Facebook has a “Family Safety Center” at [facebook.com/help/safety](https://www.facebook.com/help/safety) where users can get a wealth of information including tools and resources, teen and family safety, Facebook resources for parents, information that teachers can use to teach online safety, and additional information on Facebook safety, security, and privacy. Facebook also offers detailed safety, security and privacy tips and related information on its page at [facebook.com/security/app_268616169836752](https://www.facebook.com/security/app_268616169836752).

There are currently several third-party utilities and resources available that can help implement appropriate privacy and security settings on Facebook. On my primary computers I have Trend Micro's Titanium Maximum Security installed which offers as one of its features a Facebook privacy utility that is implemented by clicking on the “Check My Privacy” button. Trend Micro then runs a utility which checks and verifies all of the privacy settings, displaying any potential privacy threats; in my Facebook account, Trend Micro found one privacy threat suggesting that I turn off the “Instant Personalization” feature on my “App Settings” menu. Other similar utilities are available as browser plug-ins and include Facebook Privacy Watcher for Firefox (www.daniel-puscher.de/fpw/), Privacy Fix for Firefox and Chrome (privacyfix.com/start), and others. The popular technical support websites all have some form of Facebook privacy and security information. While somewhat dated, the Dallas based MakeUseOf website offers a free download (registration or “Like” required) of its 52 page “The Unofficial Facebook Privacy Manual” from its website at www.makeuseof.com/pages/download-the-very-unofficial-facebook-privacy-guide. Gizmo's TechSupport Alert.com website offers several sources of Facebook privacy and safety information. One such webpage, “Seven Tips To Improve Your Security On Facebook” is available at techsupportalert.com/content/seven-tips-improve-your-security-facebook.htm; another Gizmo directory of comprehensive Facebook (and other social media) safety information is included in its master security directory, under the “Online Services - Social Media Privacy” heading at techsupportalert.com/content/probably-best-free-security-list-world.htm?page=0,13.

By implementing the privacy and security recommendations of the above web pages and software utilities, Facebook users may greatly enhance their privacy and safety while utilizing Facebook, one of the world's primary social media networks.

WEBSITES:

<https://www.facebook.com/help/safety>

<https://www.facebook.com/security>

https://www.facebook.com/security/app_268616169836752

<http://techland.time.com/2013/04/04/facebook-privacy-settings-guide/>

<https://www.techsupportalert.com/content/seven-tips-improve-your-security-facebook.htm>

<https://www.techsupportalert.com/content/protect-your-online-privacy-terrific-new-chrome-extension.htm>

<https://www.techsupportalert.com/content/probably-best-free-security-list-world.htm?page=0,13>

<http://www.makeuseof.com/pages/download-the-very-unofficial-facebook-privacy-guide>

<http://www.daniel-puscher.de/fpw/>

<http://newsroom.fb.com/Key-Facts>

Still Holding on to XP or Windows 7?

Windows 8 is a radically new operating system that many users, consumer and business, are not prepared to adopt. Since its release last Fall, it's appeared on only three per cent of desktops. If you want to cling to Windows 7 or, more desperately, Windows XP, how long can you do so and what should you expect? Here's the scoop...

How Long Can I Keep My Windows XP or Win7?

Windows 7 users can rest comfortably until at least January 2015. That's when "mainstream" support of the OS will end, according to Microsoft. Until then, you will continue to receive both security and non-security updates (product enhancements and non-security bug fixes). If your license came with free incident support, you will get it.

But on January 13, 2015, support for Windows 7 will be scaled back. You'll still get free security-related updates, but patches will be available only by subscription. You will have until April 15, 2015, to buy a subscription to this "extended support." Warranty claims will not be honored and you will not get new features, only bug fixes.

All support for Windows 7 will end in early 2020, according to Microsoft's product life-cycle policy. After that, you will receive no security patches and money won't buy any other support. By then, you'll need a plan to migrate to a newer version of Windows, Mac, Linux, or whatever else is available in 2020.

What About Windows XP?

Windows XP is much closer to becoming an orphan. XP has been in the Extended Support phase since April 14, 2009, and all support will end on April 18, 2014. (Extended support for Vista will end in April 2017.) If you are running XP, you should start planning a migration to Windows 7 or Windows 8 real soon now. It isn't a trivial task, especially for business users.

User data and settings will transfer to a newer operating system fairly easily. But all application software will have to be re-installed. That means you may have to track down CDs, DVDs, downloaded installation files, and license keys. Some applications written for XP will be incompatible with Windows 7 or 8, wholly or in part. You should identify incompatible apps well ahead of time and find alternatives.

Clinging to an orphaned operating system is a foolish and dangerous option, not unlike driving on bald tires or an empty oil reservoir. Malware writers and hackers will increase their targeting of orphaned operating systems and you will receive no defensive patches. Some sort of disaster is virtually guaranteed.

"You'll Have to Pry it from My Cold, Dead Hard Drive..."

If you're still running XP or Windows 7, and you're determined to do so for as long as possible, here are a few pieces of advice:

Use good anti-malware protection. My related articles [Lab Tests Reveal Top AntiVirus Programs](#) and [Free Anti-Virus Programs](#) will provide some helpful tips.

Have a backup plan. If you have an old operating system, you probably have an old hard drive too. Regular backups will save your bacon if the drive fails, and will also put you in a better position to move on to a new computer or operating system when the time comes. See my tips in [Free Backup Software](#) for help with backup strategies.

Start taking inventory. My article [What's Going On Inside My PC?](#) will help you identify the hardware and software installed on your computer. If a component inside your dusty old computer fails, you'll have a parts list to help you replace it. You'll also be able to create a handy list of your software license codes, so that when Windows upgrade time finally comes, you can more easily re-install the software you've purchased, without having to buy another copy.

Is It Hard to Move to Windows 8?

The primary complaint about Windows 8 is that the user interface is completely different. Microsoft has decided that the new interface they designed for smartphones, tablets, and touchscreen computers should be shoe-horned on all desktop and laptop computers that run Windows 8. The familiar Windows desktop is still there, but it's shoved off in a corner, and they've eliminated the Start button.

Making the leap to Windows 8 is less painful if you can keep the Start button and other familiar user interface features. A number of third-party programs let you do just that. One of them is Windows 8 Start Button <http://www.windows8startbutton.com> which preserves the Start button; boots your system into the Win 7-like "desktop mode," restores familiar window and menu options, and lets you customize classic Windows and Aero modes. Best of all, it's free. Still, you may face application compatibility issues when upgrading from XP, and to a smaller degree when upgrading from Win 7.

I understand that for many users, there's just no compelling reason to switch from XP or Windows 7, when everything seems to be working fine. Windows 8 will come to them only when they purchase a new computer. I have desktop computers in my home running both XP and Windows 7, and a laptop with Windows 8. Sometime before next April, I'll retire the XP machine, buy a new computer with Windows 8, and restore all my files from backup. As for the XP software I use now, I'll try to find free alternative (preferably web-based) equivalents in the interim. As for the Windows 7 machine, I see absolutely no reason to upgrade.

Free Malware Removal Utilities from Kaspersky

by Ira Wilsker

One of the most frequent requests that I get from readers of this column has to do with removal of malware from infected computers. Most frequently, I have recommended the free versions of MalwareBytes (malwarebytes.org) and

 <h3><u>Kaspersky Rescue Disk 10</u></h3> <p>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.</p> <p>🔴 Read License Agreement before downloading.</p> <p>▸ What is Kaspersky Rescue Disk 10? ▸ Download Kaspersky Rescue Disk 10 [ISO, 250 MB]</p>	 <h3><u>Kaspersky Virus Removal Tool 2011</u></h3> <p>Virus Removal Tool is a utility designed to remove all types of infections from your computer. It implies effective algorithms of detection used by Kaspersky Anti-Virus and AVZ. It cannot substitute a resident antivirus application.</p> <p>🔴 Read License Agreement before downloading.</p> <p>▸ Differences from other Kaspersky Lab products ▸ Download Virus Removal Tool 2011 [EXE, ~100 MB]</p>
--	---

SuperAntiSpyware (superantispyware.com). I typically suggest downloading, updating and running one, and then repeating the same cycle with the other, in order to have the redundancy to reasonably ensure that the computer is free of malware. While these two anti-malware utilities, when properly updated and run, have an excellent reputation for detecting and removing malware, no single or pair of programs is absolutely 100% effective at detecting and removing malware from a badly infected computer. Fortunately for us, there is a broad selection of other competent, free utilities available

from a variety of authors that also offer the user the ability to detect and remove difficult malware.

One such company that offers a wide assortment of free antimalware utilities that can reliably detect and remove different types of malware is the Moscow, Russia, based Kaspersky. In terms of sales and users, Kaspersky is well entrenched as one of the top four antivirus vendors, producing security software for corporate clients of all sizes, small businesses, and individuals. In its 16 years as a cyber security company, Kaspersky has gone multinational with offices in 30 countries, operating in nearly 200 countries, and employing over 2700 people. While headquartered in Moscow, its corporate holding company is in the UK. Kaspersky currently provides security services to over 300 million individual users and 250,000 corporate clients worldwide.

One of the free utilities from Kaspersky that I have personally used many times to clean a badly infected computer is Kaspersky Rescue Disk 10. According to Kaspersky, "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." Kaspersky Rescue Disk 10 is downloaded as a large 250MB file in ISO format (rescuedisk.kaspersky-labs.com/rescuedisk/updatable/kav_rescue_10.iso) that must be burned to a blank CD or USB in order to make bootable media. The ISO format is not simply copied to a blank CD like a music or video file, but must be installed using an ISO image burning utility in order to make the CD bootable. While most major CD burning software offers an ISO burning option, many do not, which may necessitate a dedicated ISO burning utility.

My personal favorite is the free ImgBurn software (www.imgburn.com) which can create a bootable CD from the ISO file. For those who may need it, detailed instructions on how to create the Kaspersky Rescue Disk 10 from the downloaded ISO file and then booting the computer with the newly created CD are online at support.kaspersky.com/8093. Once the bootable Rescue Disk CD is created, and the computer booted with it, the Rescue Disk can be updated and then be used to scan, clean, and restore infected computers. Booting from the Rescue Disk is often more effective than using online or PC based security scans while Windows is loaded, as the Rescue Disk contains its own operating system; since Windows is not loaded or running, malware is more vulnerable to detection and removal, possibly greatly improving detection and removal rates. This is also an excellent method to try and recover computers so heavily infested with malware that Windows will not boot, or otherwise boot into malware that has taken control of the computer (such as the infamous "ransomware"). It may be a good practice to create one of these bootable CDs right now, and store it someplace safe but accessible, such that it is readily available in the future if it is ever needed.

Another free virus and malware removal tool from Kaspersky is Kaspersky Virus Removal Tool 2011, also called AVPTool 2011. Do not let the moniker "2011" fool you into thinking that this is some two year old product, as the utility is fully updated when downloaded from Kaspersky at www.kaspersky.com/antivirus-removal-tool?form=1. A large download of about 152MB, this utility is only intended to detect and remove malware infections that are already on the computer, and once downloaded, cannot be further updated; if future scans are necessary, a freshly updated copy needs to be downloaded again. Kaspersky Virus Removal Tool 2011 is an excellent scanner and cleaner, but only functions as an on-demand scanner, and does not provide any continuing or real time protection; Kaspersky recommends that it be uninstalled after running and cleaning an infected computer. There is still a continued need for a full-

time security utility, a function not provided by this tool. This Kaspersky Virus Removal Tool 2011, when freshly downloaded and run, is an effective way to check and verify that malware has not penetrated your existing security software and jeopardized the security of your computer.

Kaspersky also offers a large selection of free dedicated software utilities that are intended to remove specific types of malware, such as the recently endemic “ransomware”, and its more vicious cousin that also encrypts the user's computer unless a ransom is paid. These, and dozens of other malware specific utilities are freely available from Kaspersky at support .kaspersky.com/us/viruses/utility. Another form of ransomware that has appeared places a large banner across the monitor screen, blocking the view of the screen, unless a ransom is paid. Kaspersky offers a free “unlocking code” at support.kaspersky.com/ us/viruses/deblocker, which is, a “Free service Deblocker [which] helps to delete/remove banner from Desktop, unlock Windows or restore access to encrypted files without sending an SMS message.”

Many times, users want to perform a quick scan to determine if their systems are clean and free of malware; Kaspersky offers a free online scan using the latest malware definitions “in the cloud.” This Kaspersky Security Scan (usa.kaspersky .com/downloads/free-anti-virus-scan) can identify viruses, malware, and other security threats, displays information about any issues found, but does not clean any infections which may be on the computer; one of the other scanner-killers can be used to disinfect the computer. Kaspersky recently released a new version of a downloadable security scanner, Kaspersky Security Scanner 2.0 (support.kaspersky .com/us/viruses/kss2), which is a free utility designed to scan your computer for antivirus status and vulnerability detection. This Security Scanner 2.0 identifies and tests the firewall, security software, and searches for other vulnerabilities, but like the cloud based scanner, does not remove any detected malware. If any rogue security software is found, Kaspersky offers additional information and removal information on its rogue software website at support.kaspersky.com/us/viruses/rogue. A somewhat similar product, Kaspersky Virus Scanner for Mac, is available from the Apple app store (details: support.kaspersky.com/us/viruses/kvs).

For those who simply want to be sure that their computers are free of malware and other security threats, or to remove otherwise difficult to remove malware, Kaspersky has a variety of free utilities that can likely perform those services.

WEBSITES:

<http://support.kaspersky.com/us/viruses>

<http://usa.kaspersky.com>

http://rescuedisk.kaspersky-labs.com/rescuedisk /updatable/kav_rescue_10.iso

<http://usa.kaspersky.com/downloads/free-anti-virus-scan>

<http://www.imgburn.com>

<http://support.kaspersky.com/8093> (Instructions on burning Rescue Disk and booting computer with bootable CD)

<http://support.kaspersky.com/us/viruses/utility>

<http://support.kaspersky.com/us/viruses/kss2>

<http://support.kaspersky.com/us/viruses/kvs> (MAC security scanner)

<http://support.kaspersky.com/us/viruses/rogue>

Who's Driving this Bus Anyway?

by Dave Helmer

Past President and Co-Founder, Computer Users' Group of Greeley, CO

When is the last time you worried about having the latest drivers for your computer? Ever? Never? Yeah, me too. Most people just don't give it any thought beyond the initial install of a new piece of hardware, but manufacturers tend to release new drivers all the time. Even your motherboard manufacturer sometimes releases updates. Mouse drivers, NIC drivers, USB bus drivers (there's probably a joke there somewhere, but it escapes me), hardware that no one ever thinks of in their computers, that may not be running the most current drivers. And really, why should you care? Mostly because those little outdated drivers might be the cause of some significant computer problems.

For the most part, I'm a firm believer in the old "if it ain't broke, don't fix it" approach to system maintenance, but on more than one occasion, one or another of my systems will BSoD* for no apparent reason. Microsoft's pathetic approach to a diagnostic simply tells you that the problem may have been caused by an outdated driver. Well, duh ... Which one? Yeah, yeah, I know that BSoD's don't exist in the newer operating systems. But when a computer does a hard reset while you're in the middle of an hours-long project, does it really matter what you call it?

Keeping those drivers current is a nightmare, because no one really keeps track of the manufacturers and driver release numbers for everything in every computer they own. No one. Well, no one I know, or would want to know I suspect. I am usually doing good to keep my video and sound card drivers current, and yes, I do use discrete hardware plugins on my desktop systems. Motherboard sound and video is just not good enough for some of the things I use my computers for, although it is getting better all the time.

The good news is that there is a solution to this problem! Why else would I be writing this article? Actually, there have been a number of solutions to this problem over the last decade or so, but I have found none as user-friendly as a little freeware program called SlimDrivers, available at www.slimwareutilities.com. A recent article in *Maximum PC* magazine introduced me to this cloud-based utility for keeping drivers current, and it blew me away when I tried it.

Download the installer from the website listed above. Note that there are two other free utilities they offer as well, one of which, SlimCleaner, I am currently playing around with. Run the installer and when it's fully loaded, hit the big button labeled Start Scan. It's just about that easy. (Do be careful when accepting the install, as they will try to install AVG Security Toolbar into your browser, not a bad thing, but if you're not into AVG you might not want to have it auto-installed.) SlimDrivers then goes out and uses "Crowd-sourcing to spider and aggregate millions of devices" to find drivers. In English, that means it checks the hardware driver versions on your computer, matches them against the latest versions available online from the manufacturer, and presents you with a list of drivers for which updates are available. For those concerned, SlimWare Utilities is a Microsoft Gold Certified Partner, which means it should play very well with Windows. I've successfully used it on systems running Win8, Win7, Vista and WinXP, and was very satisfied with its ability to locate updated drivers on all 4 platforms. You are given the option to set Restore points before any new drivers are installed, and you can un-install or restore drivers from within the program.

At this point, the shine wears off a little bit, because you can only select one driver at a time to update. The drivers seem to download very slowly, and to be honest I end up wondering if SlimDrivers is choking my download speed as a way of enticing me to upgrade to their paid version (DriverUpdate, \$29.97/one year license), or if I am just being paranoid. And seriously, for freeware? I can take the wait. I haven't been able to discover whether or not that one license would cover all my systems, or if I need a separate license for each computer. Guess which one I would pay for... After each update, you are advised to restart your computer, and although you probably don't really "have" to do so each time, I certainly recommend it. This of course adds to the frustration of time being consumed.

Has it prevented any more BSoD's on my systems? Too early to tell, but I feel a lot more comfortable knowing that I am running the latest versions of hardware drivers on my computers. This program delivers, with a clean, easy-to-use (and understand!) interface. Learn more about it by visiting their website, www.slimwareutilities.com, and give it a shot.

*Blue Screen of Death. If you don't remember those, you probably have not been using a computer for very long.

From the March 2013 issue of Random Access, newsletter of the Computer Users' Group of Greeley, CO. Courtesy of APCUG.

On the Shelves Now: New Technology Replacing Old Standbys

by Ira Wilsker

Recently, I was one of several presenters at the Taylor Career Center's Business and Technology Summit. My topic was on the new computing technologies currently on the market that are making the existing technologies obsolete.

According to published reports, during the first quarter of 2013, PC sales (desktop and laptop) dropped 14%, while tablet and smartphone sales soared. Some of the blame for the decline in PC sales has been the lack of widespread acceptance of Microsoft's new Windows 8 operating system, as well the fact that tablet computers are generally less expensive and more portable than traditional laptops and desktops. With over a billion smartphones expected to be sold this year, along with 200 million tablets, many users have decided to forgo purchasing a new PC. Sales of PCs this year are predicted to be about 300 million, down from 353 million in 2012, and far less than Microsoft's "hoped for" 400 million PCs sold in 2013. "This is horrific news for PCs," said BGC Financial analyst Colin Gillis. "It's all about mobile computing now. We have definitely reached the tipping point."

Some pundits are predicting the slow demise of such traditional giants as HP, Dell, and Microsoft as smaller upstarts continue to erode their market shares with newer, less expensive technologies that also add enhanced portability. On the hardware side, HP and Dell are far behind the curve when it comes to technological replacements for the traditional desktop and laptop computer, while Microsoft has not captured much market share with its builds of Windows 8 intended for the portable market. As has been typical, Apple, with its successful iPad series of tablets, tends to be a leader in the introduction of new technologies. A growing threat to the established and traditional software operating systems, best represented by Microsoft's Windows and Apple's iOS, is Google's Android operating system, which has garnered a 75% market share of the operating systems of smart devices, including phones and tablets. Even giant chip

maker Intel is feeling the sting, as most of the PCs utilize Intel chipsets, and a decline in PC sales ultimately impacts Intel. In terms of the new portable smart devices becoming so popular, Intel is but a bit player, with many feisty small chip makers picking up a growing share of the CPU chip market with their sales to smart device manufacturers.

A visit to any of the local big box stores will clearly show the increasing market share of tablets and other smart devices, as they devote more shelf space to the smart devices, and much less shelf space to the more traditional laptops and PCs.

One feisty new player in the hardware market is none other than powerhouse Google, which has introduced a line of relatively low cost but highly portable devices that combine the portability of a tablet with the convenience of a traditional laptop or notebook PC. As thin as half-inch, and weighing only a few pounds, these new devices are being marketed as “Google Chromebooks”, which retail for as little as \$199, and have screens typically larger and more readable than most tablets. Unlike most common tablets, Chromebooks have a traditional keyboard and are in a form similar to a laptop. Using Google's Chrome operating system, these Chromebooks are complete and ready to run out of the box, without the need to purchase additional software. For those who want even more software, thousands of free apps (applications) are available from Google's Chrome Web Store. Included in all Chromebook models are Google Docs, which can create, read, and write office documents (word processing, spreadsheets, presentations, etc.) from and to almost all other major software formats, including Microsoft Office products (Word, Excel, PowerPoint, etc.). Other included apps are a variety of music, voice and video utilities. Chromebooks include “Google Drive”, highly secured data centers with file storage service that stores files safely online, without the need to create backups of critical files. Data files can be accessed from anywhere, and are safe and recoverable even if the Chromebook is lost or damaged.

In terms of security, Chromebooks do not require any additional security software as they use multiple layers of protection providing a “defense in depth” that is generally considered safe from malware, viruses, and other threats. At boot, Chromebooks perform a rapid self-check to verify that the system is secure and free of malware; any necessary security updates are automatically downloaded and installed, meaning that Chromebooks always have the latest security features and updates.

Many users find the boot time of traditional PCs to be somewhat aggravating, often taking several minutes; the typical Chromebook can boot in as little as 10 seconds, making its features and apps almost instantly available. Also, many PC users fail to install operating system upgrades as well as software updates; Chromebook users do not have that problem as Chromebooks automatically update themselves and their installed apps for free; there is never a need to purchase or manually install updates and software upgrades with a Chromebook. All Chromebooks are Wi-Fi equipped, and several models offer optional wireless connections through Verizon, with 100 MB of data per month for free. All Chromebooks include an interesting feature, “Google Cloud Print” which can print to many printers without the need for connecting cables.

Chromebooks are currently manufactured by Acer, HP, and Samsung, with other makers soon to have Chromebooks of their own. At present, Chromebooks are available locally at Best Buy, and online from Amazon, TigerDirect, Newegg, Best Buy Online, and HP's online store.

Another new technology which is being used to make smart devices and laptop computers more rugged as well as extending their battery life is the “SSD” or “Solid

State Drive”. Now built-in to many newer laptop and desktop computers, as well as available for installation into almost all other laptop and desktop computers, the new SSDs are much smaller in physical size, have no moving parts, require less power to operate, do not emit a lot of heat, are silent in operation, have very fast access times, and are generally far more rugged than more traditional hard drives. A typical SSD is very small and light in weight, typically measuring about 4 inches long, by 2.8 inches wide, by 0.4 inches thick, and weigh about three ounces; some are as small as 1.8 inches wide, while some are about the same package size as a 3.5 inch hard drive. Many newer laptops and desktops incorporate an integral mounting for these SSDs, and inexpensive (about \$7 - \$10) adapters are available to mount SSDs into most other laptop and desktop computers. Some newly manufactured PCs utilize a hybrid system with an SSD drive containing the operating system and other frequently accessed files, and a traditional hard drive for extended storage capacity; these hybrids often boot much faster than similar PCs can boot with a common hard drive.

Even though prices have dropped considerably in the past year, and prices are projected to continue to drop in coming years, they are still generally more expensive than traditional electromechanical hard drives, and offer less storage capacity, even though some SSDs are available with terabytes of capacity.. It is expected that as storage capacity increases, and prices drop on these SSD devices, the common electromechanical hard drives may go the way of floppy discs, and disappear from the marketplace due to obsolescence.

Considering the “gee whiz” factor when 5.25" floppies replaced 8" floppies, which were in turn replaced by 3.5" floppies; when early 10MB hard drives were scarce and terribly expensive; when colorful flat wide-screen monitors replaced older monochrome CRT monitors; when the first smart phones appeared on the market; when laptops first out-sold desktops; Pocket PC's; Palm Pilots; and other technological wonders appeared, they were greeted with vigor, and then disappeared down the trashcan of history. Do not get too attached to your Windows (or Mac) desktop or laptop with your hard drive, as they too may soon be relegated to functional obsolescence as were our Commodore 64, TI 99/4A, Atari 800, Adam, Amiga, VIC-20, TRS-80, and other popular computer types that we loved during yesteryear. Get ready to say hello and welcome new technologies and devices, as the future is already here today.

WEBSITES:

<http://www.sfgate.com/business/technology/article/Research-firm-PC-sales-plunge-as-Windows-8-flops-4424529.php>

<http://windowsitpro.com/windows/it-s-official-pc-sales-fell-q4-2012-and-full-year-2012>

<http://www.fool.com/investing/general/2013/04/12/the-pc-is-dead-and-these-2-stocks-may-be-too.aspx>

<https://www.google.com/intl/en/chrome/devices/features-different.html>

<https://en.wikipedia.org/wiki/Ssd>

Holy cow! Is this a virus?

by Linda Gonse

Editor/Webmaster, Orange County PC Users' Group, CA

I recently added a second external hard drive to my computer system. I use one for backups of InDesign files and the other one for Acronis True Image system backups. As I browsed through the files I'd saved to the drives, I ran into something peculiar. Both drives had folders with names that were long strings of random letters. And each folder contained one file: mrtstub.exe at 89KB on the Iomega drive, and MPSigStub.exe at 227KB on the Seagate drive.

Fearing these might be malware or a virus, I quickly did a Google search. Interestingly, the search turned up conflicting opinions in different forums. Some people said it was a virus and highly dangerous, some said the folder and file(s) inside were benign, some said the files were leftover from when Microsoft Malicious Software Removal Tool (MRT) was run and had not been deleted automatically, and some said Windows created them.

Although I only found one file in the folders, other people have seen as many as four at one time: mrtstub.exe, mrt.exe._p, MRT.exe, and \$shstdwn\$.req.

I found a link to information about the Malicious Software Removal Tool at <http://support.microsoft.com/kb/890830#Faq>. In particular, it gave instructions on how to remove the Malicious Software Removal Tool.

The Malicious Software Removal Tool does not use an installer. Typically, when you run the Malicious Software Removal Tool, it creates a randomly named temporary directory on the root drive of the computer. This directory contains several files, and it includes the Mrtstub.exe file. Most of the time, this folder is automatically deleted after the tool finishes running or after the next time that you start the computer. However, this folder may not always be automatically deleted. In these cases, you can manually delete this folder, and this has no adverse effect on the computer.

I also learned that MRT is not a substitute for a resident antivirus for various reasons: 1. MRT only removes malware AFTER infection, it doesn't BLOCK malware like an antivirus does; 2. MRT is designed to target a small set of malware only, while an antivirus takes care of most malware in the wild; and 3. MRT can only detect actively running malware — an antivirus can also detect dormant malware.

Microsoft's Knowledge Base (<http://support.microsoft.com/kb/890830>) also said a new version of the Microsoft Malicious Software Removal Tool is released every month. After you download the tool, the tool runs one time to check your computer for infection by specific prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection it finds.

This KB article contains information about how you can download and run the tool, and what happens when the tool finds malicious software on your computer.

Even though I did not intentionally download the Removal Tool or run it, I read that Windows Update may do that when it downloads automatic updates. Further, it uses the largest hard drive on the system to create the temp folders; and in my case, the external hard drives are the largest with each being 2TB.

The upshot of this was I checked each file's Properties and confirmed Microsoft had signed them. Then I deleted the folders and files manually and nothing bad happened. In the future, I'll disconnect the external drives before downloading or installing Windows Update.

Review: *The Artist's Guide to GIMP, 2ND Edition*

by Bill Treadwell

Member, Big Bear Computer Club, CA

GIMP is a full featured, free, open source software for graphic design and photo manipulation. GIMP contains powerful tools with a large menu of options and submenus.

When I first heard about GIMP, I down loaded and installed it. When I started exploring how to use it, I became lost and overwhelmed and did not use the software. I am a novice when it comes to using graphic design and photo software. GIMP contains a high level of complexity and many powerful tools.

The Artist's Guide to GIMP, 2nd Edition is based over GIMP version 2.8, which is the most current stable release of the free open source software. Hammel's artist guide came to my rescue.

As a GIMP beginner, I found the introductory chapter on fundamental techniques provided brief descriptions of all the menu items and icons to be invaluable resource. I continually referred back to this section to look up an icon's purpose and where to find the icon in one tool box or another.

GIMP is so rich in features that it takes determined effort to become comfortable moving around in the software package.

The major strength in Hammel's artist's guide is his step through or step-by-step

instructions for editing pictures or designing objects for use on web pages like buttons and banners. Following the examples in the artist's guide provided clear cut procedures for using the GIMP features and tools.

Hammel provided a latter chapter on creating advertisements, which could be applied to any media. Of course, this chapter further exposed additional GIMP tools for manipulating art work.

In this 320 page user guide, I am sure you will find the tools you need for your next creative photograph enhancement or for designing eye catching web graphics.

Hammel's *The Artist's Guide to GIMP, 2nd Edition* has opened the door for my GIMP use.

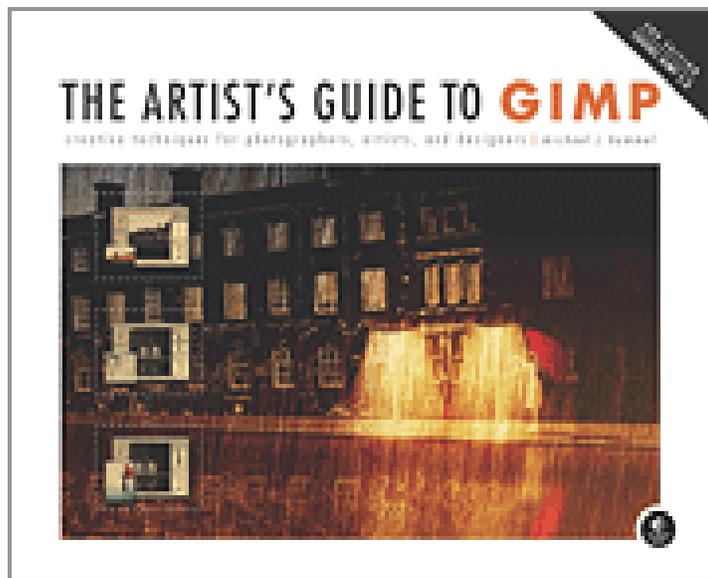
The Artist's Guide to GIMP, 2ND Edition

Hammel, Michael J. (2012)

No Starch Press, Inc. ISBN 978-1-59327-414-6

Amazon.com - \$26.36 / Kindle \$26.04

From the February 2013 issue of Bearly Bytes, newsletter of the *Big Bear Computer Club, CA*. Courtesy of APCUG.



Review: Kingston HyperX SSD

by George Harding

Treasurer, Tucson Computer Society, AZ

SSD's are a wonderful addition to the hardware library of storage devices. They are small, have no moving parts and are much faster than other storage media. On the down side, they are more expensive than other media and storage sizes are smaller than what is easily available in other media. The speed advantage is one that can be capitalized on to load one's operating system faster.

You can use your hard drive to hold and access your applications and data, or you can use the SSD for some applications, those that take longer to load.

I received a very nice 240 GB unit for review. I had tried a couple of other SSDs, but had problems of one sort or another with them. The Kingston unit comes complete with what you need to install it in either your desktop or your laptop.



The box contains the SSD, a nifty screwdriver suitable for either Phillips or slotted screw heads, a drive enclosure, a 3 .5" mounting bracket, a USB cable, a SATA drive cable and a CD-ROM with instructions and a version of Acronis software.

The procedure for a desktop is to clone your hard drive to the SSD with the Acronis software. Then you reboot from the SSD. The hard drive can be used as storage for data and applications, as usual. Another approach is to install operating system software to the SSD and boot from it.

For a laptop, the procedure is somewhat different. You first remove the internal hard drive and install in its place the SSD. The internal hard drive is mounted in the supplied drive enclosure and attached to the laptop with the USB cable. You clone the hard drive as before.

I had a few difficulties with these installations. First, I tried the desktop approach, but the Acronis software would not clone the hard disk to the SSD. The latter was grayed out in the destination choices, so I took the alternate approach and loaded Windows 8 to the SSD and was able to boot to it.

In the case of the laptop, I was not easily able to remove the internal hard drive, so I gave up on that approach. Kingston's Tech Support will be helping to solve my difficulties – more later.

The HyperX is a well-put-together kit and should be usable by most anyone. The instructions are very clear, with pictures each step of the way. The Acronis software is reliable.

About: Kingston HyperX SSD

Vendor: Kingston

www.kingston.com

Price: \$275, \$203 @ Amazon

From the February 2013 issue of eJournal, newsletter of the *Tucson Computer Society*, AZ. Courtesy of APCUG.

Sources of Support for Linux Open Source Software

by Bill Wayson

Linux SIG Moderator, Channel Islands PCUG, CA

An important responsibility of any user of computers and technology is knowing where to get help. This month I will (again) discuss some of the places users of open source software can find help and how to identify whether or not the help offered is any good. There really is no shortage of people and places willing to provide support, most of which welcome people willing to help others. Here are some suggestions to get you started.

The Internet

The best source of support for Free and Open Source Software (FOSS) is the Internet. The Internet is where members of the open source community (which includes you, the user) meet. The Internet is the one open forum that can provide real-time feedback on FOSS as it is updated and patched. Tap into this knowledge base through your favorite Web search site. Creative search terms, such as an error message, can result in just the solution you are looking for.

The types of information you will find fall into three categories: FOSS-oriented sites; FOSS vendor sites; and FOSS mailing lists and discussion forums. Many FOSS-oriented sites are great gateways to FOSS information. Try Linux Online (www.linux.org) and Linux Questions.org (www.linuxquestions.org). Many more sites like these exist, and each deserves a look. One that merits special attention is The Linux Documentation Project (www.tldp.org). This is the home of the HOWTO collection, a community-maintained FOSS documentation project. Topics covered there range from setting up a three-button mouse to a Web server. Some HOWTOs may be a bit old, but others actively follow the latest developments.

Most companies that create and distribute Linux have their own websites. If you search on Linux Mint, openSUSE, Red Hat, or Ubuntu, you should be able to find their home pages easily. Usually you will find links to knowledge bases, support forums, and bug tracking. Purchasing a vendor's official Linux distribution usually entitles you to toll-free

phone and email support, and access to reserved web sites.

Searches for support will invariably return links to messages in mailing lists and discussion forums. The online forum, basically an online conversation, has become a standard support offering of almost all providers of software. People post their problems in the hope someone can help and will post the answer. These postings and solutions are immortalized in an archive of the discussion. Find a good one and make it a regular online hangout.

On Your PC

Linux installations include a great deal of documentation on Linux itself and FOSS. If you have installed the source code for Linux, you'll find information in `usr/src/linux/Documentation/`. The information there can be helpful if you are having trouble with a specific piece of hardware. Application documentation can be found

under /usr/share /doc. This information will range from very terse to extremely deep. You may also find howtos installed under here.

You may find “Help” icons on your Linux desktop or application menu — most distributions include a help system. And don’t forget the “man” (short for manual) and “info” (short for information) pages.

Use a terminal window under Linux to enter the command “man man” and “info info” to get started. The man system is the traditional source of application and utility reference information. The newer info system, which is slowly replacing it, sports hyperlinks and better document organization.

User Groups

User groups can be great sources of information and support. CIPCUG has its Linux SIG. Nearby are the Simi/Conejo Linux Users Group (www.sclug.org) and the Ventura County Linux Users Group (www.vclug.org). A trip to one of their meetings could be worthwhile. To find other user groups, simply search for “linux user group” and a city. This is sure to return results for any city of any size.

These groups often have very good websites and mailing lists, and I have never had a problem joining their mailing lists.

Magazines and Books

A trip to the computer section of any large bookstore will offer you many, many books that cover all sorts of subjects that are Linux- and open source-related. Books give you the ability to learn at your own pace. Some series to look for are the O’Reilly books, the SAMS Teach Yourself in 24 Hours series, and No Starch Press books. Before you go to the bookstore, think of three or four real questions that you have. Look at several books and see how easily and understandably your questions are answered, and choose the book that does this the best. Also look for magazines that cover Linux, like Linux Magazine (www.linuxpromagazine.com) and Ubuntu User (www.ubuntu-user.com). These are sold at the larger bookstores.

Information is there just for the asking It is true that there are very few instances of “1-800-LINUXHELP” support, and most of these cost money. But once you start using the resources described above, you will discover that there is no shortage of support for, and information about, Linux and other FOSS. As you become comfortable using these resources, the perception that you are on your own when you use Linux and FOSS will fade and disappear as a reason to not give Linux and FOSS a try. It all starts with looking.

Courtesy of APCUG.

Giving Internet TV a Try

by Gene Olson

Member, ICONPCUG, Long Island, NY

After getting the Cable bill, I wanted to reduce the rates by having Internet TV (and cutting out Cable). After reading about “Satellite Direct,” which seemed like it was better than other Internet TV software – I bought it. It cost \$50 over the Internet. I would NOT recommend using a regular credit card.

PROS:

1. It does give you a lot of channels.
2. Lots of channels are in English.
3. They do provide music channels.
4. The quality on most channels is great.

5. Some channels are the same channels on Cable TV.
6. It has a nice menu to select Video by country.
7. It has a nice ability to Search Video from any country.
8. The channel changing is fairly quick.
9. Even some of the foreign channels are in English (Brazil TV had the Beatles in English).
10. It does have the ability to get some channels from HBO, Showtime, Cinemax, etc.
11. It's better for a person who knows foreign languages to get other country channels.
12. Lots of channels are from Satellites.
13. The one-time \$50 fee is not bad to try the product, get connected to Internet TV and without a monthly charge.

CONS:

1. It does not allow you to install it on any other computer (even one you own).
2. It didn't provide as many channels as they indicated (3500).
3. Many channels are from foreign countries.
4. Some channels don't load.
5. I can't get all the channels that I can get on Cable TV.
6. Some channels have software in front of it that you have to get around.
7. Some screens are blank.
8. Some channels are slow (requiring 10 seconds to connect).
9. Some content on some channels repeat.
10. Some channels are not online all the time (understandable for other countries in a different time zone).
11. Some channels the audio runs, but the video stops, and/or the video jumps.
12. Not good if you only know English (like me) and there are many foreign language channels.
13. It seems the same advertisements are on multiple channels – seems to be from "Satellite Direct."
14. Once installed, the software wants you to upgrade to their Premium Package at \$5/month.

I read an Internet review that some Internet TV software overflows the buffer and downloads viruses and malware to your computer. They were right, after three days – I had a Trojan on a computer that never gets viruses and is not used for the Internet. I will now have to run constant full Virus Protection scans on my computer more often.

Review: The software could be written a lot better, without viruses, without advertisements, without distracting screens. They don't tell you what you get with \$5/month more premium package. I would not recommend it, primarily because of the viruses. But if you do use it, use on a spare computer (one that you can reformat).

From the November 2012 issue of The ICON Graphic, newsletter of the

Check the security of your password instantly.
howsecureismypassword.net

Netted by the Webbys
Cherry-Pick the Internet

Dragdis Bookmarks Photos, Videos, and Text

The Internet has gotten smarter. Bookmarking hasn't. Ironically, it's an old-school browsing maneuver that's finally bringing bookmarks up to speed.

Dragdis is a plug-in for Chrome, Firefox, and Safari that lets you literally drag anything on the page (or the page itself) and drop it into a magically appearing bookmarks bar. Dig a photo? Drag it. Think a video is cool? No need to find the source, just drag it. Like a piece of text? Highlight and get dragging.

When you start dragging an item, a drawer full of folders appears on the right-hand side of your browser. Drop your haul in the correct folder (you can create as many as you need) then go back to browsing.

Back at your personal Dragdis homepage, you can search your stockpile of bookmarks and even use tags and notes to categorize them.

If nothing else, you should check out the impressive Dragdis website. In addition to dragging, they've made scrolling pretty fun, too.

Need stuff to drag? You'll find a bunch of save-worthy content right here.
www.dragdis.com

Society News

Help's Half Hour Notes

Led by Dan Rothfuss
Notes by Jan Rothfuss

Q. Using Windows XP and, after using for 15 minutes, he gets a warning about insufficient space.

A. There may be a couple of issues. Your disk may be full. He should run Microsoft Cleaner (under Windows Tools) to clean out some of the unnecessary files.

Q. One member knows someone who has lost their address book. He followed the directions that were provided in the monitor but this seems to have broken the address book. He also has another issue as his printer is no longer recognized.

A. Arpad said that he might be able to discover the problem. Perhaps they can get together after the store closes.

The Lighter Side

