

PC Post



Official Newsletter of the
Modesto PC User Group.
Modesto, California

30 YEARS OF USER HELPING USER

March 2012, Volume 30.3

Inside this Issue

Windows 8 - Exciting & Challenging	2
Change of Allegiance - Does the Antivirus You Use Really Matter?	3
New Google Privacy Policy - Do You Want to be Tracked?	5
Product Review: Digitz® Wireless Ezmouse	8
What the heck are hiberfil & pagefile	9
Geek Busters! Part Deux	12
Ads	14
Officers	15

The group meets at 6:30 p.m. at Denny's Restaurant, 1525 McHenry Ave., for its Random Access Special Interest Group featuring questions and problems members are facing. At 7:30, following dinner, the presentation will start.

BOD Meeting - April 4, 7pm at Ridgeway's

Windows 8 Consumer Preview Evaluation Copy Build8250 A free download from Microsoft

The President/Webmaster Jim Goodman downloaded Windows 8 as a iso image format then burned the image to a DVD. (At Denny's we do not have a good enough connection to download Windows 8 iso image and burn to a DVD).

The computer has an AMD Athlon 64 X2 3800+ 2 GHz Processor with 1 GB of memory. No problem installing Windows 8 on this computer.

If Microsoft doesn't do something soon, Apple is going to take over the consumer market with their iPad. So, Windows 8 is a big deal to Microsoft.

Windows 8 is the upcoming version of Microsoft Windows that follows Windows 7. It features a new Metro-style interface that is designed for touchscreen, mouse, keyboard, and pen input. It also adds support for the ARM processor architecture in addition to the previously supported x86 microprocessors from Intel and AMD.



Windows 8 - Exciting and Challenging

By John Pearce, Member, Pikes Peak Computer Application Society, Co
March 12 issue, Bits and Bytes
www.ppcompas.apcug.org / [glenihan \(at\) comcast. net](mailto:glenihan@comcast.net)

The Microsoft Development Team for Windows 8 has been writing a blog about its development. The first post was in August, 2011; the frequency varies from a few days to a few weeks. I have often wondered why certain design decisions are made in the Windows OS. The blog attempts to discuss some of those issues as related to Windows 8. <
<http://bit.ly/xlUCi8> >

Based on what I have read in the Microsoft blog and in the computer trade press, I think Windows 8 will be both exciting and challenging. Windows 8 will run on legacy x32/64 hardware as well as the ARM processor found in tablets. The blog posting related to the ARM processor called this Windows on ARM or WOA.



You will have your choice of Windows 8 on a desktop, laptop, net book, ultra book, or tablet.

The look and feel of the Metro interface will be the same across all the hardware platforms. The difference is the physical control of the interface. If you want to use the touch interface with your desktop PC, you will need a touch enabled screen, otherwise you will still use the mouse. You can also revert to the old style desktop if you must.

In some ways, Windows 8 reminds me of the transition in Windows that happened with Win 2000. A benefit of melding the Windows 98/Me product line with the NT 3/4 product line was a way to run games that wanted to have direct control of the display screen. The dark side of the Win 2K release required new drivers for devices because Microsoft changed how drivers interact with the OS.

Windows on ARM generally requires new code. Porting most of the existing applications is not allowed because the ported applications would negatively affect battery life and would require more system resources than programs developed specifically for WOA. And there is the issue of designing the interface for Metro rather than the traditional Windows desktop.

The Windows Consumer Preview (otherwise known as a Win 8 beta release) was available by the end of February. The release is reported to be open to anyone who wishes to download and install the software. The hardware used to run the preview must meet the minimum requirements for Windows 7.

Microsoft is saying there is lots of work to do before the first release candidate is ready. There are few hints about the Windows 8 release schedule. It appears Microsoft is aiming for a grand slam event with Windows 8 on tablets (ARM processors) and on x32/64 hardware.

Change of Allegiance - Does the Antivirus Software You Use Really Matter?

By Greg Skalka, President, Under the Computer Hood User Group, CA
March 2012 issue, Drive Light
www.uchug.org / president (at) uchug.org

I just switched to a new antivirus program. I'd been a loyal user of my previous program for over five years, which seems like an eternity in the ever-changing computer software business. I've wondered for some time if it mattered which brand I used. Although there are probably dozens of antivirus programs available, some of which are even free, I have only ever used four. Am I using the best one? Is there a best one? Would I be wasting my time trying to determine the best one? And is what is best relative to my needs anyway?

I was surprised at the results of an informal survey taken at one of our recent general meetings. Our membership appears to use a wide variety of the available antivirus offerings. Around a dozen different vendors were being used by our members, with no one source having more than 10% of the market in our group. With the market apparently so fragmented, can one brand really be that much better than the others?

I don't deny the importance of computer security. It is a common tenant of cyber security that every computer should run an antivirus program to protect against those threats. Microsoft believes this so much that every version of Windows since XP performs checks to see that an antivirus program is installed and that the virus signatures are not out of date. I'd just like to see proof that the antivirus software is doing its job.

One of my problems with antivirus software is that, at least in my experience, it seldom finds any viruses. I've tried to be diligent in my regular computer maintenance, running antivirus and anti-malware software once each week and keeping the signatures updated. My anti-malware software will often find some kind of spyware or malware on one of my computers to quarantine or delete, but from all the probably hundreds of hours I've spent running antivirus scans, I've yet to find a virus. I do know viruses still exist out there in the cyber world, as I have seen others have them. My daughter had a virus on her laptop last year, and this month we found the Conficker worm on some network servers at the company I work for. Since I've not found any, could I be running just a placebo antivirus program?




I guess the effectiveness of antivirus software is something we may have to take on faith. I've never seen comparisons or reviews of antivirus software that evaluated the ability to detect or remove particular threats.

Usually the software's rating is based on less essential but more measurable parameters like ease of use, cost or manufacturer's reputation. With new virus threats appearing constantly (or so we are led to believe), how can a program's ability to quickly recognize something new be evaluated in advance? Selecting an antivirus program

might be similar to choosing a religion, in that all you have initially is your faith in your choice, and you won't likely find out until much later whether you chose correctly.

originally started out (over a decade ago) using Norton Antivirus, as it was one of the first and few of this type of program on the market. They also offered a lot of rebates on their products, so I could usually get my antivirus every year for free. I really liked the Norton Utilities, and so it was not long before I was using Symantec's Norton SystemWorks suite. I also really liked the ZoneAlarm firewall, and so used their free version for many years alongside the Norton suite. Eventually, however, Symantec came out with their own firewall program, and they made a decision that has me soured on their products to this day. Symantec made their Antivirus product incompatible with the ZoneAlarm firewall, probably to promote their own Norton firewall. This made me have to choose between them, and ZoneAlarm won. I don't think I've purchased a Symantec product since.



 Around this time, ZoneAlarm came out with their own security suite, ZoneAlarm Internet Security Suite. It combined my favorite firewall with antivirus and anti-spyware. It was also usually available periodically for free after rebate (my favorite kind of software), so I used their suite on all my computers for at least five years. The ZoneAlarm antivirus never really impressed me, but at least it worked well with their firewall, and so I had faith that it was protecting me.

In the last year, however, the ZoneAlarm antivirus turned into a real nuisance. It became a drag on my computer's resources, slowing it down considerably while updating and while scanning. Every time my computer was started, the suite tried to check for updated antivirus signatures. This process took minutes to complete, and occupied the computer to such an extent that it was not possible to use it until the update was completed. This became very annoying, as it slowed my computer just as I was most interested in using it. If I wanted to boot my computer quickly to look up something on the Internet, it added additional minutes to my search time. It also suddenly went from a few hours to overnight and more to run an antivirus scan. I even tried (unsuccessfully) to disable the antivirus updates. Finally I had enough and decided to look for a new antivirus program. This also coincided with the end of my ZoneAlarm ISS subscription and the apparent end of their rebate deals.

During this time I had also used McAfee's antivirus briefly on a new computer that came with a free trial, and used it on the computers provided by my employer. I didn't think it was anything special.

A trusted reference was the deciding factor in my selection of a new antivirus program. Our group's webmaster has been using ESET's NOD32 antivirus software for many years, and had nothing but good to say about it. He claimed it used little hard drive space and ran quickly with little impact on computer performance. I considered using it in conjunction with the free version of the ZoneAlarm firewall, but a rebate deal on ESET Smart Security persuaded me to try another firewall program as well. I bought two of the three-user packs, and figured I was set for all my computers for the next year.

I soon found out why the ESET Smart Security 4 suite was offered at a discount, as within a month Smart Security 5 was released. I was allowed a free upgrade to version 5, but found upgrading from 4 to 5 had issues. It was much better to install version 5 from the web (using my normal activation information), as it allowed the installation on a drive other than the boot drive. The firewall also seemed to work better this way. I'm still learning about ESET's firewall, but their antivirus seems to live up to its reputation as easy on resources. I guess I have something new to have faith in.



New Google Privacy Policy - Do You Want to be Tracked?

By Ira Wilsker, Member, Golden Triangle PC Club, TX; Columnist, The Examiner, Beaumont, TX; Radio Show Host, Mondays, 6-7pm CT, KLVI.com
iwilsker (at) sbcglobal.com

WEBSITES:

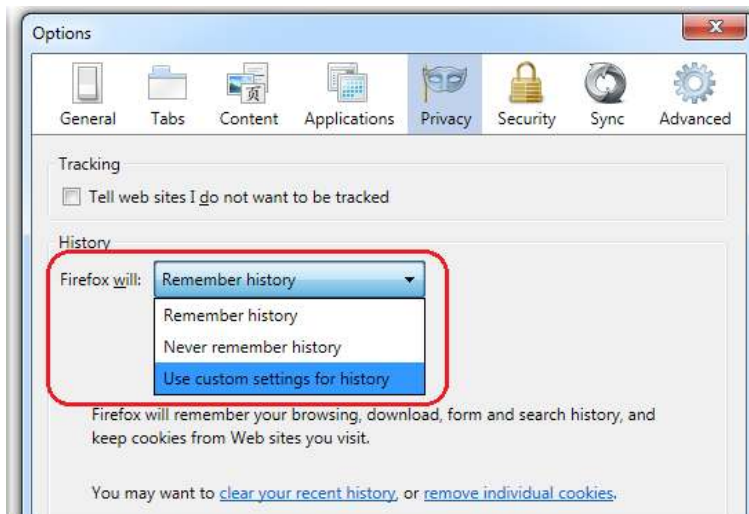
<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/02/18/BUSO1N9ASP.DTL>
<http://www.foxnews.com/politics/2012/02/18/lawmakers-target-google-over-privacy-laws/>
<http://arstechnica.com/tech-policy/news/2012/02/google-hit-with-ftc-complaint-says-circumventing-safari-privacy-features-accidental.ars>
<https://www.google.com/intl/en/policies/privacy/preview/>
<https://www.google.com/intl/en/policies/>
<https://support.mozilla.org/en-US/kb/Cookies>
<https://support.mozilla.org/en-US/kb/Disabling%20third%20party%20cookies>
<http://donottrackplus.com>
<http://www.youtube.com/watch?v=D-cwcWiB8mU> (YouTube Video about DNT+)
<http://www.ghostery.com>

Recently there has been some controversy in the media and in the blogs about Google's new privacy policy, Google overriding the Safari browser's "do not track" feature, and other potential privacy issues. As many internet users are aware that the "free" online services such as Google and Yahoo! are advertiser supported, receiving compensation from advertisers for the banner ads that appear on every page, paid placement in search engine results, and other revenue sources, most users are unaware that their browsing habits are also tracked with the information used (sold) to advertisers.

There are several ways that web services such as Google track users, and these include a variety of "third party" cookies (small text files mostly used for tracking purposes), web beacons (1 pixel graphic files that are virtually invisible to the user), IP tracking (your browser typically broadcasts its IP address), and other methods. Some browsers, such as Apple's Safari block third party cookies by default, while other browsers offer the option to block or

allow third party cookies. In Firefox, third party cookies can be blocked or managed by going to TOOLS (in the menu bar) - OPTIONS - PRIVACY - and then pull down the menu at "History - Firefox will:" and select "Use custom settings for history." Another selection will

appear that allows the user to accept third party cookies by checking the box, or by refusing them by unchecking the box. If third party cookies are accepted, the user can then use the pull down menu to keep them until they expire (from hours to decades), automatically delete third party cookies when closing Firefox, or be asked what to do with each cookie. With Internet Explorer the default medium-high privacy setting in IE blocks most dangerous third party cookies by default. If desired, the IE user can manage his own privacy by



clicking on TOOLS - INTERNET OPTIONS - PRIVACY - ADVANCED and then the user can select to accept, block, or prompt whenever third party cookies are encountered. The reason why Internet Explorer does not block all third party cookies is aptly explained on a Firefox help page, "Some websites (e.g. Microsoft's Hotmail, MSN, and Windows Live Mail webmail) use third-party cookies for purposes that are not necessarily privacy concerns, and disabling third-party cookies may cause problems with those sites."

Many of the antispyware utilities, such as SuperAntiSpyware and MalwareBytes, when run routinely scan for and delete third party tracking cookies during a security scan. Rather than using a security scan to delete tracking cookies that may already be on the computer, which have been busily sending the users' browsing habits to third parties until they are deleted, it may be better to stop or minimize tracking before tracking can take place. Some browsers, such as Firefox, have a "Do Not Track" feature that tells websites and their advertisers that this user does not want to be tracked. In Firefox, this feature can be quickly and easily enabled by clicking on TOOLS - OPTIONS - PRIVACY - and checking the box "Tell websites I do not want to be tracked." Even though the user explicitly asks not to be tracked, many websites and advertisers do not honor the request, while others will respect the users' wishes. Enabling the "Do Not Track" feature does not apply to beneficial cookies, such as shopping cart cookies, or cookies containing saved login information. Some advertisers question blocking their content which was automatically determined by the tracking and third party cookies, alleging that it reduces the "user experience" by not allowing user relevant advertising to be displayed. If you ever wondered how banner ads that somewhat applied to your personal interests were displayed in your browser, it was likely based on the third party tracking cookies that were previously placed on your drive.

In order to help protect your online and browser privacy, there are several free useful browser plug-ins or add-ons that block or otherwise provide control over these third party cookies and other tracking tools. One of my personal favorites is "DNT+", or Do Not Track +. This free utility, available for download at donottrackplus.com, works on both Macs and PCs with the most commonly used browsers, including Google's Chrome, Firefox, Apple's Safari,

and Microsoft's Internet Explorer. DNT+ has a cute, animated video which explains what it does and how to use it online on YouTube at youtube.com/watch?v=D-cwcWiB8mU. As a quick experiment while typing this column, after installing DNT+, I connected to CNN.com, and then clicked on the green DNT+ icon on my browser tool bar. DNT+ reported that it blocked nine trackers, including one social network, three advertising networks, and five companies that were tracking visitors to this particular CNN webpage. With some irony, the San Francisco Chronicle webpage with the story about Google's tracking controversy contained its own trackers; and even dozen trackers, including three social networks, three ad networks, and six other companies tracking visitors to that particular webpage. Since it works on Mac and Windows, with all of the major browsers, and is free, Do Not Track + may be a good utility to protect your privacy.



Another interesting and free browser utility that can display a variety of tracking utilities hidden on a webpage is Ghostery, available for free download from ghostery.com. According to the Ghostery website, " Ghostery sees the invisible web - tags, web bugs, pixels and beacons. Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity." Ghostery empowers the user to decide which, if any, trackers and related privacy threats are to be blocked or allowed. After Ghostery is installed, anytime a webpage is opened, a red box appears in the top right corner of the browser window which displays the tracking cookies, web bugs, scripts, and other tracking devices embedded on that webpage that are rarely disclosed to the viewer of that webpage. Ghostery is a free browser plug-in that works on Firefox, Chrome, Safari, Opera and Internet Explorer. As an example, on another CNN page that I just opened, Ghostery found 10 tracking tools, all detailed by clicking the ghost icon on the browser toolbar. Once the selection of tracking tools is displayed, Ghostery can provide detailed information about each, and allow the user to permanently block that particular tracking device.

With all of the controversy about Google's new privacy policy, and the various methods of user tracking embedded in most of the websites that we visit, it would be a good practice to manage third party cookies, enable browser "Do Not Track" features (although many websites routinely ignore that request), and install both Do Not Track + and Ghostery. While most websites track users for legitimate commercial purposes, and intend no harm, there is always the slight possibility that that same information can be misused. I put Ghostery and DNT+ on all of my computers, because I do not like my internet usage to be tracked; you should consider doing the same.

Ira Wilsker is the Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVI News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.

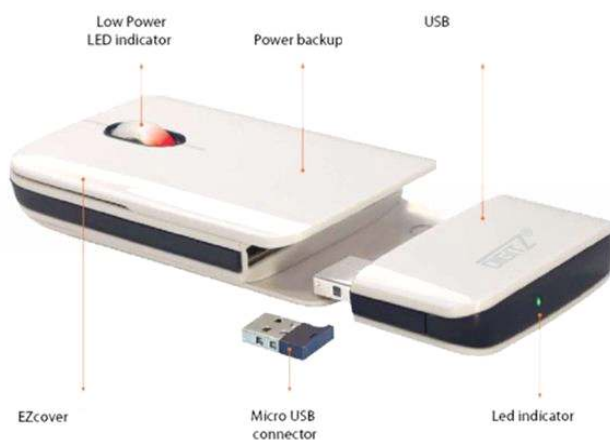
Product Review: Digitz® Wireless Ezmouse

Reviewed by David Kazmer, Member, SCV Computer Club, CA

April 2010 issue, the DATALINE

www.scvpcg.org / scvcomputerclub (at) gmail.com

Many years ago I got my first notebook PC and found out about all the gadgets it would take to be prepared to use it at any location. There were so many cables that the notebook case almost wouldn't fit under an airplane seat. Since then, the new technologies that emerged, especially wireless, have taken a lot of the bulk out of the case. One of the remaining bulky items was the mouse, until I discovered the wireless Digitz EZmouse.



The first attraction was the flat, slim design, perfect for my notebook case. It is a small rectangular shape just 4" long by 2.1" wide, by .7" thick and weighs just .132 lbs, but that is just the tip of the iceberg. It is very comfortable to use, as you don't have to arch your hand as with other mice. The shape fits under my hand very nicely, and the two long skids on the bottom glide very smoothly on just about any surface. There are the standard two buttons and scroll wheel, plus pressing down on the scroll wheel is the third button.

One of the amazing features is that it does not require any conventional batteries! The unit contains two lithium-ion polymer batteries, one internal and one attached through a USB connector. The external battery, about 1.25" by 2.25", fits into the rear of the mouse and detaches for charging from any PC USB port. A red LED by the scroll wheel will blink when the external battery has about 15 minutes left. A complete charge would take about two hours and will operate the mouse for about five to six weeks of normal use. While the external battery is detached and charging, the internal battery will keep the mouse operational for up to three days. To facilitate possible charging access space problems, the USB connector on the external battery is attached by a swivel, and there is an LED at the back of the battery to indicate the progression of the charging. Life expectancy of the batteries, based on normal use, is about eight years! This innovation is impressive.

Stored in the mouse is the wireless 2.4G nano-receiver which plugs into any computer USB port. Also, if the mouse is not used for about 20 minutes it will go into a sleep mode to save the battery; just click the mouse to wake it up. The optical sensor is 1600 DPI for high accuracy. A felt carrying bag is included. The mouse is both PC and MAC plug-and-play compatible.

Ready for the icing on the cake? The top cover can be replaced by one of your own design by ordering it from Digitz and sending them a JPG picture of your choice! Check www.digitzgroup.com for more details and an informative video. If the display does not appear in English, just click on the small American Flag icon.

SCV Computer Club Rating (0-5, 5 being best)



Digitz EZMouse

www.digitzgroup.com / www.ezmouse.com

info@digitzgroup.com

\$49.95 (Free shipping – USA and Canada)

What the heck are hiberfil and pagefile

By Linda Gose, Editor/Webmaster, Orange County PCUG, California

February 2012 issue, Nibbles and Bits

www.orcopug.org / editor (at) orcopug.org

One day while purging unnecessary and unused files on my Windows XP computer, I spotted two massive files on the C:\ drive that perplexed me. One was hiberfil.sys at nearly 3.5 gigabytes! And, the other was pagefile.sys at 2 gigabytes!

I did not delete them right then and there. First, I checked them out on Google. As it turns out, both of the system files serve a purpose.

Hiberfil.sys is a file the system creates when the computer goes into hibernation mode. Windows uses the file when it is turned back on. If you don't need hibernation mode and want to delete the file you need to turn the hibernation option off before Windows will allow you to delete the file.

The file size depends largely on the size of active RAM in the computer as the contents of the file are basically a RAM image. That explains why the file was so large. My computer has 4G of RAM — although it only recognizes 3.25 gigabytes.

I couldn't see a need to have hibernate enabled on my computer so I disabled it by unchecking the Enable Hibernation box in Power Options in the Control Panel. (The procedure for turning hibernation off is significantly different between Windows XP and Vista.)

The next time I rebooted, though, my UPS scolded me for not having hibernation enabled. The UPS unit used that as storage space in case the power goes out and battery power has to kick in.

I was careful to research pagefile.sys before taking any kind of action that might compromise it.

Good thing, too. Pagefile.sys is the virtual memory file Windows uses. Typically, when installed, Windows sets the size of the file at around 1-1/2 times the physical memory size.

However, the size may vary depending on the amount of free disk space when the file is created and other factors. The default size generally works fine but it can be changed. Windows uses this file for its normal operation, but if you really need the space you can delete it after turning the virtual memory option off. Just be aware that this can cause extreme instability in Windows — even causing it to stop working. Yikes!

Back in the old 3.11 Windows days, a file like this was called a swap file. Windows used the hard disk space even then to simulate extra memory. A swap file helped when printing large documents, among other uses.

Not surprisingly, experts advise leaving pagefile.sys alone and to look elsewhere for files to delete!

Using Windows Task Manager to Get Out of Potential Harmful Situations

By Terry MacLennan, Member at Large, Sauk Computer Users Group, IL
Originally published in The Computer Connection, the newsletter of the
Sauk Computer Users Group
www.saukcomputerusersgroup.org / [wcseniorcenter \(at\) gmail.com](mailto:wcseniorcenter@gmail.com)

There is an easy method of getting your computer out of two situations of potential harm. To do this, we will use the operating system's built-in program called the Task Manager.

The first situation is when you have too many programs running at one time and the computer locks up. This lockup can also be caused by a single program that for one Reason or another, fails to run properly. Reaching over and hitting the power button may seem to be your only option but there is a much better choice.

The second situation occurs when you are on a webpage and one of those realistic looking but totally phony "security alerts" pops up on your monitor screen warning you of imminent danger of viruses and other malware that "it" has detected on your computer. These scare popups trick many naive people into clicking on them only to find out that now their computer truly is infected and control has been lost. You are totally helpless when you have clicked on one of these so-called "security" scam programs.

You absolutely must not click anywhere on these pop-ups including buttons that say something to the effect of "No Thanks," "Decline" or even "Continue Unprotected." But, instead of clicking one of those, you may decide, almost instinctively, to click the "X" in the corner of the pop-up box. Doing any of these actions is almost like turning your house alarm off, opening the door and saying "come on in" to the masked bandit standing outside. Paying the "bandits" for their "security program" which is holding your computer hostage is an extremely poor choice. Do you really want to pay the thieves with your credit card and its number?

But you are now stuck in a situation where you may try to click off the web page by clicking on its "X" in the upper right hand corner. But you soon find out that that won't work as you first need to close the window (the pop-up in this case) that is on top.

Hard shutting down the computer by using the power button may seem to be your only option but again there is a better alternative.

Your best friend in both situations is the Task Manager. To open this built-in program, press and hold the CTRL and ALT keys with your left hand, then tap the DEL key with your right hand.

In Win XP, this will automatically open the Task Manager while with Windows 7 it will take you to a page with a list of options. Click the bottom option and it will open the Task Manager which looks nearly identical to the XP one. From here, everything is the same for both systems.

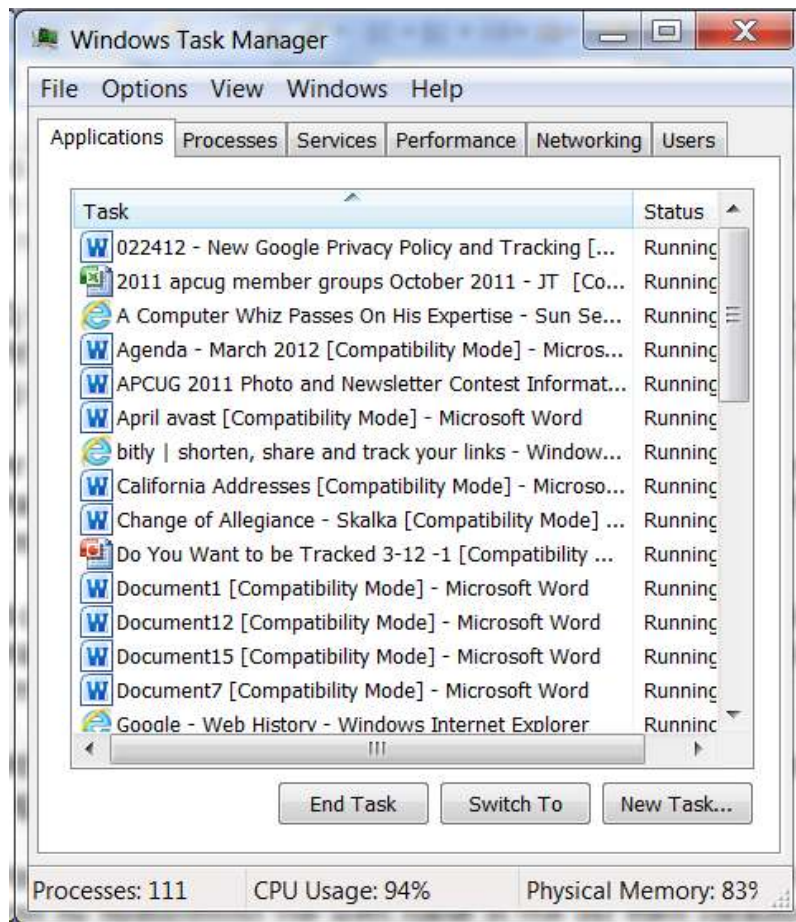
Along the top edge of the Task Manager is a row of tabs. Click the Applications tab, if it doesn't happen to automatically be on that tab. When you have opened it up, you will see a listing of all the programs and web pages that are running.

If your computer is locked up, look for any programs that are "Not responding." Click the program one time to highlight it then click on End Task at the bottom. This should close the nonresponsive program and free your computer.

If the computer remains locked up, use the same method to close all of the remaining Programs that are running then shut down as you would normally. Everything should be back to normal when you reboot the computer.

A hard shutdown with the power button is absolutely the last resort as this could potentially damage files.

To close a web page with the dangerous fake security warning pop-ups, use the same method by highlighting the web page in the list then clicking End Task. This will safely shut down the web page with its pop-up without installing the malware "security program."



Geek Busters! Part Deux



In this week's [Tech Tip](#) we'll look at some common "techy" misconceptions that we'd like to dispel with "**Geek Busters!**" - sending myths into hiatus! Without further preamble, I give you our items for this week's Tech Tip Geek Busters!

#1 Facebook wants to charge you money for its service



It seems like a week doesn't go by that the rumor mill churns yet again that [Facebook](#) wants to charge you some kind of fee for its service. Basically, put them out to pasture - Zuckerberg and company loves your information that we all (maybe too) freely give out to want to charge us for the privilege of paying him to give it. So, feel free to grouse about the latest changes to the format but know that for now and into the foreseeable future, **Facebook is content to**

just be happy mining YOUR data.

#2 Apple "invented" the PC (or the MP3 player; or the Tablet computer)

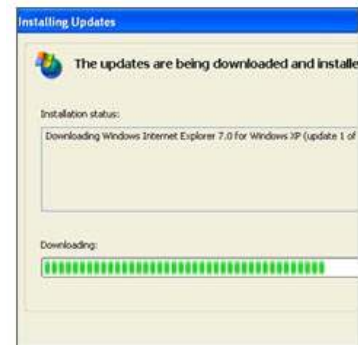


All of these are an astounding no. Apple marketed one of the first Do It Yourself (DIY) personal computers (for an astounding \$666.66 (no, Steve Jobs is not the Antichrist either) and had a strong foothold in the market well before IBM unleashed its version of the PC onto the world a few years later - but many companies marketed computers well before Apple (some notable examples are the MITS Alter; HP 9100 (and even if you want to dig further back you can find examples like Honeywell's Kitchen computer and even the DIY Simon that you could purchase the plans for).

Ditto for MP3 players (remember the Genica Tavarua) and **tablet computers have been around for ages** (it just took Apple to make them fun and bring them out of the business world and into our lives - with tons of knock-offs coming on its heels screaming "me too! me too!").

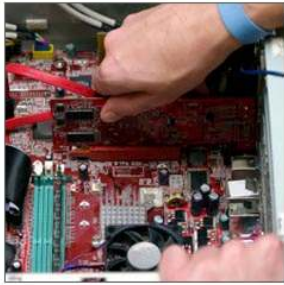
#3 Running Windows Updates will ruin my computer

Actually, quite the opposite may be true - if you avoid running updates, especially security updates, you put your computer at risk. While it is true that every once in a while an update has some - unexpected consequences - for the most part you are better safe than sorry running the update. However, it has to be said that if you update an entire operating system, then there is the strong possibility that many of your favorite programs will not migrate well to the newer version of the operating system (not that this has ever held me back - thank goodness for Virtual Machines and especially for XP Mode on Windows 7)



#4 Dell (or Apple, or HP, or Acer; or “insert companies name here”) manufacturers their own computers

While some companies may still ASSEMBLE some of their computers to order, most computer companies no longer own any manufacturing facilities or make their own computers. There are a few exceptions, but for the most part, large computer companies have third party manufacturers build their computers (which is why some of the largest BUILDERS of computers are companies that you may have never heard of, such as Quanta Computer, Compal Electronics and Hon Hai Precision (aka, Foxconn Electronics)).



Be assured that the computer you are probably reading this Tech Tip on was more than likely not actually MADE by the company that is on the label. This is one of the big reasons computers are basically considered commodity items (yes, even that shiny Apple PC - rolling off the same assembly line with Dell, HP, etc.) and tend to have similar repair rates (which also means that they also tend to use many of the same OEM parts and components as well). **This doesn't mean that your computer was made poorly; or even that one computer may be “better” than another - it just means that they are all pretty**

much the same.

In Conclusion

We hope you liked this week's Tech Tip! While urban legends and myths run rampant in the tech arena, rest assured that we here at Tech Tips have your back and are ready to beat back the hounds of ignorance and set a world on fire with Geek Busters!

From Ray Nichols

If you have items you would be willing to donate for our club drawings, they will be gratefully accepted. Be sure to wear your name badge for the drawing.

Please also remember to bring your used magazines, books, videos, DVD's, and cassettes for distribution to Veterans in our area. If you have old household or device batteries, or used CFL (Compact Fluorescent Lamp) bulbs, bring them for legal recycling (it is against the law to dispose of them in the trash). Old Cellphones can be converted to Telephone Calling Cards for overseas Military Personnel. Old eyeglasses will be turned over to the Lions Club for reissuing to needy





For Information about our website host and how you can get on board:

Click on this link info@fire2wire.com

Need help hooking up that new PC, or installing DSL-Cable? Call Jim Goodman, \$60.00 for as long as it takes.579-0122 jgood99@sbcglobal.net Modesto, Ceres Area

Cyrano Writing & Editing
 When you need help putting it in words, call Cyrano.
 (209) 523-4218; 499-5401
Resumes, letters, applications, articles, newsletters, press releases, theses
 Elizabeth Leedom

Modesto PC User Group Officers

President	Mike Kumler	531.2262	president@mpcug.net
Program VP	Jim Goodman	579.0122	sig@mpcug.net
Secretary	Terry Fix	524.8062	secretary@mpcug.net
Treasurer	Barbara Cameron	522.1389	treasurer@mpcug.net
Director-at-Large	John Selover		dal@mpcug.net

Appointed Positions

SIG Coordinator	Jim Goodman	579.0122	sig@mpcug.net
Press Relations	Elizabeth Leedom	523.4218	programvp@mpcug.net
Membership	Terry Fix		membership@mpcug.net
Webmaster	Jim Goodman	579.0122	webmaster@mpcug.net
Editor	Judy T aylour	661.252.8852	scvjudy@usa.net

PC Post

Editor Emeritus: William "Doc" Holloway – 1920-1996

Editor Emeritus: Claude Delphia

President Emeritus: Bud Bondiotti – 1950 - 2008

Join The Modesto PC User Group

To join MPCUG (or just get more information about us, go to our Website and fill out the new member form or mail your check to: MPCUG, P.O. Box 5122, Modesto, CA 95352-5122. Membership is just \$24 a year and includes 12 issues of the PC Post along with participation in all meetings and events. You will also receive E-mail advising you of extra events or news.

The PC Post and Editorial Policy

The PC Post is published online 12 times per year and is available to all group members as a membership benefit. Annual group membership dues are \$24.00. Opinions expressed in PC Post do not necessarily reflect the opinions or views of the members as a group or the Board of Directors. The PC Post encourages group members to submit articles for publication. We would like to have articles which deal with the writer's experience with computer hardware and software or digital photography. An article may deal with any computer-related subject provided it contains no libelous or offensive material. We can't use information copied from other publications without written permission except for quotes. Articles should be submitted in unformatted MS Word or RTF text. Proofread and run your spell checker; watch for special upper and lower case in brand names. If you want to include a graphic, please send it as a jpeg attached to the E-mail submitting your article. Please note in the article where the jpeg should be placed. We reserve the right to edit articles for length or to improve readability. Longer articles may be published in several parts. We will not knowingly promote unlicensed businesses. Letters to the editor are encouraged. All articles and letters to the editor should be submitted to the editor via E-mail as an attached file (Word or rtf). Please include your name, day and evening phone numbers.