



THE WYSIWYG



\$3.00

January 2016

Volume 28, Issue 1

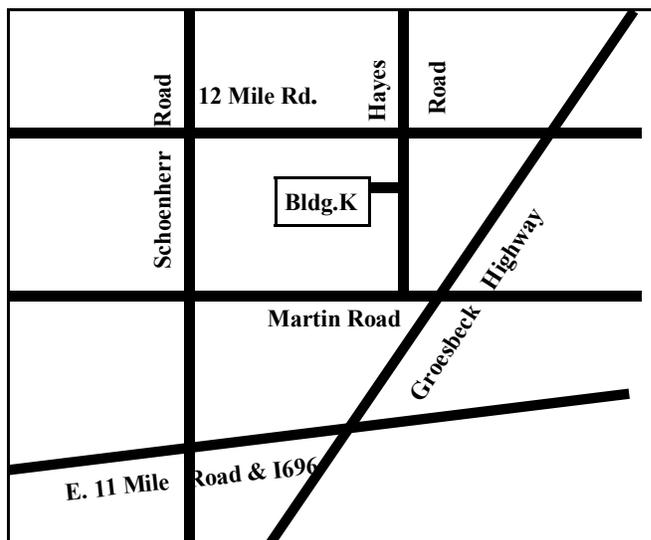
STERLING HEIGHTS COMPUTER CLUB

PO Box 385

Sterling Heights, MI 48311-0385

**MAIN MEETING: TUESDAY JAN 5
6:30 PM (changed from 7:30)**

Macomb Community College
South Campus
14500 E 12 Mile Road, Warren
John Lewis Community Center
(Building K)



IN THIS ISSUE:	
About SHCC	2
The President's Pen	3
Door Prizes	3
Save Money By Buying "Open Box" Goods	4
The Tip Corner	6
Holiday Shopping Season Opens With New Malware Targeting Credit Cards, And Android Tablets Factory Infected With Malware	8
How To Stream TV	10
Microsoft Upgrading Windows 10 - May "Automatically" Upgrade Windows 7 and 8.1 to Windows 10	11
Where To Get Instructions For Your New Devices	13
SHCC Emergency Cancellation Procedure	13
WYSIWYG Web Watch	14

This Month's Main Meeting Topic:

"New life for an old XP computer: Convert it to Linux - revisiting the live demo" presented by member Paul Baecker

NOVICE SIG Meeting:

Tuesday, January 19
starting at 6:45 at the
Clinton-Macomb
Public Library, in
Conference Room C

The SIG will plan to meet every other month, at this location, if people continue to attend.



Clinton-Macomb Public Library

The Library (Main Branch) is located at 40900 Romeo Plank Road in Clinton Township, on the east side of Romeo Plank, south of 19 Mile and Cass Roads, at the intersection of Romeo Plank and Canal roads (south-east corner).
(Tel. 586-226-5000.)



Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding to become a member or not. Meetings include the main meeting and SIG. July and August don't count since there is no main meeting. Membership includes admission to all SHCC functions and the newsletter. Membership is open to anyone. It is not limited to the residents of Sterling Heights.

DUES: \$25/YEAR

CLUB ADDRESS: PO Box 385, Sterling Heights, MI 48311-0385
CLUB E-MAIL ADDRESS: Info@SterlingHeightsComputerClub.org
CLUB WEB PAGE: http://www.SterlingHeightsComputerClub.org

Resource People:

Family Tree	Rick Schummer
Firefox	Don VanSyckel
FoxPro	Rick Schummer
General Computer Questions	Jack Vander-Schrier
Hardware	John Rady
MS Publisher	Rick Kucejko
MS Word	Rick Schummer
Spreadsheets	Rick Schummer

SHCC Coordinators:

Associate Editor	Rick Schummer
Door prizes	Don VanSyckel
Greeter for visitors	Jim Waldrop
Newsletter publisher	Rick Kucejko
Novice SIG	Paul Baecker
Program Coordinator	Mike Bader
Publicity	Patrick Little
Resource People	open
PC SIG	Jack Vander-Shrier
Welcome & check-in desk.	Jim Waldrop
Web Site	Don VanSyckel
Web Watch column	Paul Baecker

Contact Information:

Paul Baecker	586-286-2314	webwatch@sterlingheightscomputerclub.org
Mike Bader	586-447-6683	mbbader@flash.net
Rick Kucejko	248-879-6180	rick@kucejko.com
Patrick Little	586-264-1497	pblittle@wideopenwest.com
Rick Schummer	586-254-2530	rick@rickschummer.com
Don VanSyckel	586-731-9232	don@vansyckel.net
Jack Vander-Schrier	586-739-5952	jvanders@comcast.net

(Call Jack after noon)

2016 SHCC Officers

President: Don VanSyckel
 V. President: Mike Bader
 Secretary: Rick Kucejko
 Treasurer: Paul Baecker

Four Month Meeting Schedule:

JANUARY 2016

5 - SHCC – “New life for an old XP computer: Convert it to Linux - re-visiting the live demo” presented by member Paul Baecker

6 - COMP meeting
 3 - SEMCO meeting
 19 - Novice SIG

FEBRUARY 2016

2 - SHCC – Main Meeting
 3 - COMP meeting
 7 - SEMCO meeting
 ? - PC SIG

MARCH 2016

1 - SHCC – Main Meeting
 2 - COMP meeting
 6 - SEMCO meeting
 ?- Novice SIG

APRIL 2016

5 - SHCC – Main Meeting
 6 - COMP meeting
 3- SEMCO meeting
 ? - Novice SIG

Other Computer Clubs:

As a member of SHCC, you can attend meetings of other clubs where we have reciprocating membership agreements, at no charge.

Computer Club of Marysville and Port Huron (COMP)

Time: 1st Wednesday, 7:00PM
 Place: Mackenzie Bldg, Room 201, St Clair Community College, Clara E McKenzie Library-Science Building, 323 Erie St. Port Huron, MI (810) 982-1187
 Web Page: http://www.bwcomp.org
 Reciprocating: Yes

South Eastern Michigan Computer Organization (SEMCO)

Time: 2nd Sunday at 1:30PM
 Place: Altair, 1820 E Big Beaver Road, Troy, MI 48083
 (248) 840-2400
 Web page: http://www.semco.org
 Reciprocating: Yes

Royal Oak Computer Club

Time: Every Wednesday at 12:30
 Place: Mahany/Meineger Senior Community Center 3500 Marais Ave. Royal Oak, MI 48073
 248-246-3900
 Reciprocating: No

Newsletter submissions are due 10 days before the club meeting, but the earlier the better. They should be sent to :
 WYSIWYG Publisher
 5069 Fedora, Troy, MI 48098
 OR at the e-mail addresses: newsletter@SterlingHeightsComputerClub.

© Unless stated otherwise, all materials contained in this newsletter are copyrighted by the Sterling Heights Computer Club. License is hereby granted to other clubs (non-profit) to reprint with credit.

The President's Pen

by Don VanSyckel



I want to start by wishing you a Happy New Year and may you have an enjoyable one.

As I write this it is still before Christmas so I don't know what Santa is bringing me but there probably won't be much tech stuff. My Santa leaves all the tech stuff to me so I never get tech surprises. One thing that keeps popping up and I do mean popping up is Windows 10. I use Win 7 Pro on both my desktop and laptop and as soon as I log in there's a Microsoft pop up encouraging me to sign up for Windows 10. I have a problem with this intrusion into my privacy with an advertisement that I have to repeatedly refuse. Once possibly, but not over and over again. I find this obnoxious and Microsoft is not winning any friends in my court.

Why is Microsoft trying so hard, too hard if you ask me, to push Windows 10? They're giving away Windows 10. I learned a long time ago that there's no free lunch or commercial software. So not only is Microsoft giving away Windows 10 they're expending a lot of energy (and therefore money) to push Windows 10. So you have to ask yourself, where's the pay back? I don't care how many of you can't see the pay back and therefore think there isn't one. There's got to be a pay back and since we can't see it, it just means we're going to be ambushed (surprised) with it when it happens.

Then there's the spy rumors about Microsoft using Windows 10 to harvest information about you. Granted the rumors now include that Microsoft might or have extended the spying down into Windows 7. Early reports were dismissed by many as rumor. Later reports from usually reliable sources generally agree that Microsoft 10 out of the box is doing some data harvesting but it is difficult to know who to believe. There are tips avail-

able on the web for how to turn off the harvesting.

Please read the article 'Microsoft Upgrading Windows 10 - May "Automatically" Upgrade Windows 7 and 8.1 to Windows 10' by Ira Wilsker which is reprinted in this issue of the WYSIWYG. This author reports how Microsoft is planning to trick people into loading Windows 10. This will be done by masquerading the Windows 10 upgrade and a standard update for the Win 7 or Win 8 system you are currently running. To call version change of windows a standard update borders on criminal. If you have automatic updates turned on and you are presented any questions, read them carefully and don't let Microsoft steal your Windows from you.

To quote Mr. Wilsker, "According to several published reports, Microsoft has expressed concerns that the rate of Windows users upgrading from the older versions of Windows to Windows 10 has slowed, and this decline in the rate of people upgrading to Windows 10 may cost Microsoft substantial potential revenues." He mentions "substantial potential revenues" that Microsoft will reap from all of us upgrading to Windows 10 but doesn't go into detail of just how this will come about. This parallels what I stated above that Microsoft has something up its sleeve to harvest a profit from the free Windows 10 upgrade. Has the world gone mad? When something sounds too good to be true, it is.

After all this and throw in Microsoft's planned underhandedness, I won't upgrade until I understand what it's going to cost me, in the long run.

I hope everyone had a great Christmas holiday and enjoyed welcoming in the New Year. Remember the meeting

starts at 6:30PM and end about 8:00. This month's meeting will be interesting. SHCC member Paul Baecker will be demonstrating and discussion of. and programs for Linux. See you Tuesday.



Last Month's Meeting

Last month SHCC member Mike Bader presented "Windows 10 Privacy and Security Options". Mike did a great job with an evolving topic. Many tips and reference web sites to simplify the use of Win 10.



Member Ads

Ads are available free to SHCC members, and are limited to computer related items for non-commercial purposes. Any ad shall be a maximum of twelve newsletter lines of text.



Door Prizes

Door prize drawings are held at regular club meetings. The winner's circle for December included:

Ralph Osinski won Network Backup

Paul Baecker won a stereo headset

Louise Manning won a power strip

Warner Mach won a flashlight

Richard Jackson won a pro sound speaker

Mike Bader won a pen

Bill Appleberry won DVD-R's



Save Money By Buying "Open Box" Goods

by *Ira Wilsker*

WEBSITES:

<http://www.cowboom.com>

<http://www.techforless.com>

http://www.amazon.com/s/ref=nb_sb_ss_i_1_8?url=search-alias%3Daps&field-keywords=warehouse+deals+by+amazon

I like bargains, and I like to save money while shopping. While the granddaddy of all bargain days, Black Friday, and its younger cousin, Cyber Monday, are past, some people might like the selection and opportunity to take advantage of bargains at times other than these mega-shopping events. For those who might be willing to forgo a little personal vanity, some of the familiar retailers have websites devoted to often deeply marked down items that have been returned, had shipping damage, or had been refurbished to like-new condition, sometimes with the same warranty that the same new, unopened item may have had. Consider the fact that both brick and mortar local retailers, and the large online retailers, sell massive amounts of merchandise; it is inevitable that a percentage of that merchandise will be returned for a variety of reasons ranging from a refused delivery, to shipping damage to the outer package, to the item being defective and returned for replacement. Reputable sellers will always clearly disclose the reason for the markdown, present an accurate description of the current condition of the item, guarantee the description, state if the item has been refurbished to "like new" condition, disclose any warranty, and typically offer free (shipping paid) returns if the consumer is not satisfied with the marked down merchandise.

In recent weeks I ordered some merchandise that was posted on these

reputable "open box" websites ranging from a factory refurbished Lenovo laptop (not the latest model) that was marked down to about 70% off retail, as well as some mundane items such as some new premium brand wiper blades which were in perfect condition, but had some damage to their outer packaging, thus were available for two-thirds off the regular price. While I have been a regular buyer of these marked down goods when they are available, over the past year I have had two returns. In separate transactions months apart, I had a factory refurbished laptop (not the one that I recently purchased) that came with the same warranty as a new laptop, but had a battery that would not hold a charge; the seller immediately sent me a prepaid shipping label, and issued a full refund as soon as the return was received by the shipper. The second item that I had to return was purchased "Open Box" from a different major seller, and was a combination keyboard and case for an iPad, which would not link via Bluetooth with the iPad; again the seller sent me a prepaid shipping label, and provided an immediate refund when they received the item back. While anecdotally these were two "Open Box" items that were returned, considering all of my online purchases, the return of these two items was not out of proportion with my returns of absolutely "New in the Box" items, which I have also had to return in recent times.

The national chain BestBuy, known primarily for its electronics, media, and computer sales, is no different from any other big box retailer, in that a percentage of items sold are returned for a variety of reasons. While BestBuy sometimes has some clearly labeled and marked down "Open Box" items on the shelf in the stores, it also has an online outlet store that often has a wide selection of often deeply marked down outlet style goods. BestBuy's online outlet is

"CowBoom" (cowboom.com), and has a prominently posted policy, "The Great Deals, No Bull Promise, Close-out pricing everyday." According to the CowBoom website, "CowBoom offers quality new, refurbished and pre-owned products at everyday low prices. Our products are in top condition, with each pre-owned and previously out-of-box item personally inspected by CowBoom's technicians. Expect big savings by shopping at CowBoom." In order to reduce the hesitation and risk of purchasing its merchandise, CowBoom states, "15-day money-back guarantee. At CowBoom we want to make sure you are completely satisfied with your purchase. Any product we sell can be returned for a refund within 15 days of receipt. We offer pre-paid shipping labels so your return is hassle-free."

CowBoom continuously has a very large, and ever changing inventory of computers, audio and video equipment, televisions, mobile and cellular phones and accessories, cameras and camcorders, household electronics and a variety of other merchandise for home and office. Among the recognized name brands represented by the assortment of merchandise at CowBoom are Apple, Canon, Nintendo, Bose, Nikon, Hewlett Packard, Sony, Samsung, and other well known manufacturers. CowBoom also offers a daily email with the deal of the day, which is a deeply discounted, often name brand item; today (as I type this), it is an "Amazon Fire HD Kids Edition 6in 8GB - Black/Blue, Was \$149.99 Now \$39.99 + Shipping." This ruggedized tablet for children has a four and a half star rating from its users, strong parental controls, and access to Amazon's extensive library of age appropriate movies, TV shows, music, books, Android apps, and games. While much of the content available for this tablet is free from Amazon, if anyone in the family has an Amazon Prime account, all of the content then becomes available at no additional charge. Since this Amazon tablet is a "Daily Deal", a different

product will likely be available on other days. For those looking for some potentially exciting deals on CowBoom, the website also has a selection of name brand goods that are being auctioned to the highest bidder.

One of the best kept secrets about online bargain hunting is Amazon's Warehouse Deals. According to Amazon, the Warehouse Deals shopper can, "Find deep discounts on open-box, like-new, and pre-owned products." As I type this, Amazon is listing 541,866 items in its warehouse store, and states that, "Every item (is) hand checked and graded, Available for Prime & Free shipping, Backed by Amazon Customer Service, (and has a) 30-Day Return Policy." Currently listed on the Amazon Warehouse Deals website under the heading "Our Best Deals", includes a new, \$250 all leather briefcase style laptop bag marked down to \$59 with free shipping, and a new \$160 7" Android tablet for \$39. Other "Best Deals" include a 42% markdown on select "Open Box & Used Laptops", up to 59% off of "Open Box Wearables" including smart watches, half-off select open box digital cameras, up to 48% off of a selection of open box and used unlocked cell phones, up to 67% off of open box and used smart phones, 45% off of coffeemakers, and dozens of similar "Best Deals". By category and quantity, the largest selections of products available from Amazon Warehouse Deals includes books (83,756 books available in the Warehouse Deals), electronics (60,384 items), automotive (47,796 items, not including the windshield wiper blades that I recently purchased), tools and home improvement (44,935), home and kitchen (44,597), sports and outdoors (37,161), and clothing and shoes (29,179). Amazon Warehouse Deals can be located directly by entering "Amazon Warehouse Deals" in the search box on any Amazon page, and then utilizing the "Deals" page menu or search system. While that method may be totally adequate to satiate the bargain hunter, my

personal preference to locate "Warehouse Deal" priced items is to perform a routine Amazon search for a particular product, and then from that product's page click on the link that shows alternate sources for that product, including any under the "Used" tab; if there are any Amazon Warehouse Deals for that particular item, they will be listed under the "Used" heading. My personal preference when buying items under the "Used" banner is to purchase those listed as Amazon Warehouse Deals, rather than from unknown third party sellers; while sometimes slightly more expensive, I know that Amazon has inspected and rated the individual items, the description and condition is most likely accurate, I can get free shipping (I have an Amazon Prime account), and that Amazon will stand behind the purchase.

Another excellent resource for open box and refurbished items is "Tech for Less" (techforless.com), a Colorado based seller with a large selection of these discounted products. Tech for Less specializes in open box and refurbished goods from major manufacturers, with a 30 day money back guarantee, and a comprehensive "low price guarantee". Tech for Less will price match both before and after the sale, if a lower price is found on most other online and physical stores, including BestBuy.com, Overstock.com, TigerDirect.com, Newegg.com, Staples.com, OfficeDepot.com, Target.com, HomeDepot.com, Lowes.com, Amazon.com, Frys.com, Apple.com, Microcenter.com, Sears.com, OfficeMax.com, Rakuten.com, Dell.com, Crutchfield.com, HP.com, Walmart.com, and others. In order to get the difference rebated from Tech for Less, "Just send us an email with your order number, a link to the lower price, and a note that you'd like to apply our Lowest Price Guarantee."

During the past year, from Tech for Less, I purchased an Epson all-in-one printer (refurbished), three extra handsets and bases (all in new condition)

for my cordless phone, and a refurbished modem for my broadband service. Being a careful shopper, I compared prices, warranty, and shipping costs, finding that for these items, Tech for Less had the best deals. Tech for Less sells almost all of the major brands, including Apple, Canon, HP, Panasonic, Sony, and others. They carry a good assortment of laptops, desktops, monitors, TVs, portable audio and MP3 players, printers, digital cameras, camcorders, drives and other storage devices, tablets, servers, and many other products. Most items sold by Tech for Less have the same warranty as a new item, but are available for up to 75% off of the retail price for the same new item. The consumer can often choose the degree of the discount for many of the items by choosing a combination of "condition and pricing"; as an example a particular Toshiba laptop that I was considering is available with free shipping in many "conditions" such as "New - Inner Seals Intact Condition", "New - Open Box", "Factory Refurbished (Restored to manufacturer condition, may show limited signs of use, manufacturer warranty)", and "Refurbished - with manufacturer's warranty". Each lower condition is available at a lower price, which allows the potential buyer to balance the condition with the price, but regardless of condition, all of these laptops had the manufacturer's warranty.

If hunting for bargains, there may be no need to wait for Black Friday or Cyber Monday. If willing to accept a deeply discounted open box or refurbished item, often with the same warranty as a new item, that may be the way to go.

This article was reprinted with permission of the author, Ira Wilsker.



The Tip Corner

by Bill Sheff, Lehigh Valley (PA) Computer Group, Pennsylvania
www.lvcg.org nsheff@aol.com

Hacking

How do you know if you have been hacked, and what can you do about it?

You usually know when your e-mail or social media account has been hacked when you start getting calls and e-mails from friends asking you why you have changed your status to single, or your endorsement for Romanian Viagra has just arrived, or some other equally stupid message has been received by lots of people you know. It feels bad, but it has happened to most of us at one time or another. The good news is that you have not been specially picked to be hacked. We are just not that important. Even so-called safe sites can possibly be the culprit if they have been hacked. These sites can be sources of bad attachments or downloads,

The culprit can be a data-stealing Trojan. It's an awful feeling, but you can recover. The worst case scenario is that quite possibly someone now has all or part of your log-in information, and any site using that password could now be available to them.

So rule number one; if you feel you have been hacked you need to **change your e-mail password immediately**. All of your password-protected secure sites are potentially in danger. In a perfect world you'd change the password for every secure site as soon as possible. But this is easier said than done. You may not even remember all the sites that you've signed up with. Start with financial sites and other important sites, then rack your brain to come up with as many others as you can. And rather than start using the same password for many sites, this might be the time to get a good password encryption program. There are a few very good ones out there that are free. One that we have discussed previously is KeePass, and another one is

LastPass. They will generate random secure passwords.

While not too many people do it, it might not hurt to drop a line to tech or customer support just to let them know what happened. There is not too much they can do, but they might be able to suggest something. Also make sure your antivirus and malware programs are up to date and run a full scan. Use CCleaner which will also clear up problems with your registry.

Finally, for the really uptight user some people suggest you reformat your PC and start over. Perhaps it is not a bad idea, but I personally think that is overkill. Just make sure you have the latest updates for your operating system and all installed browsers and browser add-ons.

Double-check that your antivirus or security suite is fully up to date, and run the most thorough scan it offers. Don't assume, though, that your antivirus will root out all problems. After all, it didn't stop the initial hack. Get a second opinion. Temporarily disable your installed antivirus's real-time protection and run a scan using one or more of the available free antivirus tools. Focus on those that specialize in cleanup. Even with all of the above, there is no guarantee that it won't happen again. Run your antimalware programs about once a week, and be careful when using public computers.

What is encryption?

Since we mentioned password encryption above, let's talk a little bit about encryption.

Encryption is the process of securing information by transforming it with an algorithm into a form that can only be readily translated by those that know the algorithm used to make it. Early simple encryption used a simple letter by letter substitution. We see them all

the time in puzzle books. More complicated systems use various other methods of hiding data, even electro-mechanical devices such as the Enigma, and today's on-line encryption utilize 127 digit prime number algorithms as the method of tying together your computer with a secure site before data is passed. Encryption has historically been used in government correspondence, especially in the military, but since the rise of the computer and the internet, encryption has become an important part of securing vital information such as passwords and files, and preventing identity theft. We will limit ourselves to just looking at Computer password encryption.

We make up a password on our computer so that the web site knows it is really us. So the first line of defense is not to have a password that can be guessed at by someone trying to get into your account.

We call a password weak if it is simple words. Hackers can run through every word in the dictionary in seconds. But passwords may still be vulnerable to guessing strategies. People often use parts of real words in passwords, or use words or numbers that are familiar like addresses or birthdays. This makes passwords easier to remember, but also much easier to crack. Using the same password for many different programs and internet sites is also common for ease of use, but again, this makes passwords more vulnerable. For maximum protection, use a different string of random characters for each password, or better still use a password encryption program like the ones mentioned above. The more characters and the more different characters and symbols used in a password, the stronger it is to protect against a hacker.

Once you have your password and enter it onto a site, the password goes through an encryption process that changes the characters used into a string of characters that is usually much longer than the password itself

and will appear to be completely random. Most password encryptions work as a one way check for password validity: the algorithm used always transforms a given password into the same string of characters. When a password is entered, it is run through the algorithm, and the encrypted string of characters produced is compared to the encrypted password that is stored, and if they match, the password is accepted. Good encryptions will transform a given password into a character string that is nothing like the string produced by the same password when a typo is made.

Weak encryptions that use simple algorithms produce character strings can be attacked directly. Stronger encryptions can still be cracked through volume, or brute force attacks where each possible password is tested. As mentioned above strings of prime numbers are used to help keeping the pipeline between you and the site from being invaded. Today, those algorithms are very strong, so the weak link would be the password you are using to start the encryption process. Keep your passwords long, keep them varied and most important of all keep them safe from prying eyes. Don't keep your passwords list on your computer. Keep it on a USB Thumb drive that is not attached to your computer. Preventing access to your password is the best way of keeping your data safe.

Setting Up a New Computer

Whatever the reason, at one time or another we go out and buy a new computer. Perhaps we just want to graduate beyond Win XP, or finally decide to try out Win 8.1 or 10 to see what the hoopla is all about. Regardless of the reason, here are a few pointers to get your computer working as good as you can get it before you even start. Of course we want to use our new computer right out of the box, but these few tips will help make your PC a fast sleek operating machine.

First thing you want to do is make the back-up disks. There is a small emer-

gency section on the hard disk that has the appropriate software. Once you have those disks made, you know you can always get back to the original computer as it came right out of the box. And of course, you have a good back-up program to periodically make a clone of your machine, right?

If you are a purist, before you even use the machine, you can go out to the web (with another machine) and get all updated drivers from the actual retailers. Windows usually provides drivers for audio and video but getting the latest from the retailers might provide other and sometimes better options.

Get rid of the Garbage! Every new machine comes with a lot of programs pre-installed called bloatware. Many are programs that give you a trial period and then after six months or so, you have to buy them. If you are going to install your own office suite, get rid of the "trial" version of Microsoft Office suite or any of the other trial programs you know you are not going to use. Otherwise, you will be plagued by nagging screens popping up asking you to purchase something. If you don't think you will use, get rid of it. It is still out there on the net anytime you change your mind.

One program to help get rid of the bloatware is PCDecrapifier. This program automates the process of cleaning out known bloatware. Then open the Control Panel, head to Programs > Programs and Features, and work your way through the list of currently installed programs, removing anything you're not likely to use. Then go to the task manager (In Win8 it is Ctrl + Shift + Esc) and hit the Startup tab, and disable any background programs that you don't want to run when Windows launches. (Prior systems use msconfig in the start menu. You will find dozens of programs that can be disabled, which will free up system memory and resources for other applications as well as speed up your boot time.

Next, run Windows Update to get all the necessary components and security patches up to date. You should make sure you click on the Automatic file updates so you never miss a necessary update.

Install your apps. Once you have the machine completely updated it is now time to install your favorite applications. Make sure that they are compatible with your machine. You may want to try out a program called Ninite which can automate installing a number of popular applications.

Finally, it is time to install the security and antivirus tools. And then install Secunia Personal Software inspector which automatically keeps all of your programs up-to-date.

Now that you have done all of the above, back up to an external drive using Windows' built in imaging tool or some other third party program that will do the job.

This will give you a head start on reinstalling in case something goes wrong in the future. And, continue to do backups of one type or another to keep your machine as up-to-date as you can make it.

That's it. Enjoy your new PC.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.



**If your e-mail or mail address changes, please e-mail:
secretary@SterlingHeights
ComputerClub.org**

Holiday Shopping Season Opens With New Malware Targeting Credit Cards, And Android Tablets Factory Infected With Malware

by Ira Wilsker

WEBSITES:

<http://www.isightpartners.com/2015/11/modpos/>

<http://bits.blogs.nytimes.com/2015/11/24/researchers-track-tricky-payment-theft-scheme/>

<http://finance.yahoo.com/news/sophisticated-scam-targets-retailer-payment-191352635.html>

<https://www.cmcm.com/blog/en/security/2015-11-09/842.html>

<http://www.esecurityplanet.com/mobile-security/android-tablets-sold-on-amazon-infected-with-cloudsotarojan.html>

<http://www.cmcm.com/article/share/2015-11-09/840.html>

<http://www.cmcm.com/blog/en/security/2015-11-11/843.html>

This last Christmas season has been as busy for cyber security professionals as it has been for bargain shoppers. While there have been several stories in the national and local media about shopping safety and security, cyber crooks are also well aware that that the seasonal shopping frenzy creates illicit financial opportunities for those ingenious enough to create malware to again attack our "POS" (Point of Sale) payment systems, as well as to infect popular Android tablets with malware at the time of manufacture.

It was approximately two years ago that we heard about the massive credit card data breaches at Target, Home Depot, and dozens of other major retailers. Most of those well publicized data breaches occurred because a well written piece of malware was able to

infect the POS devices that most of us use at checkout to steal our debit and credit card data. While there have been many subsequent data breaches and thefts of credit card data since the massive attacks two years ago, none have reached the scope and degree of damage of the combined "Black Friday" attacks of 2013. Now, at the height of the 2015 holiday shopping season, there is some evidence that a new, more sophisticated, type of malware may be spreading through the retail channels that could repeat or surpass the sheer numbers of credit and debit card numbers stolen in the previous massive attacks. On November 24, a Dallas based cyber security company iSIGHT partners disclosed this new threat in a blog post "ModPOS: Highly-Sophisticated, Stealthy Malware Targeting US POS Systems with High Likelihood of Broader Campaigns" (<http://www.isightpartners.com/2015/11/modpos>).

According to the iSIGHT blog posting, "The threat intelligence experts at iSIGHT Partners have analyzed the most sophisticated point-of-sale (POS) malware we have seen to date. ModPOS, which is short for modular point-of-sale (POS) system, is a comprehensive malware framework. The actors behind the ModPOS software have exhibited a very professional level of software development proficiency, creating a complex, highly functional and modular code base that places a very heavy emphasis on obfuscation and persistence. Thus, ModPOS can go undetected by numerous types of modern security defenses." Preliminary reverse engineering of the malware code has shown that the source of the malware code is probably Eastern European in origin, and is explicitly written to not just capture the magnetic stripe data that was purloined in such large numbers in 2013

and subsequent data thefts, but to also steal the data from the newer "EMV Chip and PIN" secured credit and debit cards now coming into wide use, as they were supposed to provide greatly enhanced security. These new EMV (Europay-MasterCard-Visa) Chip and Pin credit and debit cards were designed to make it very difficult for cyber thieves to profit from stolen credit card data, as they did in the massive "Black Friday" attacks of 2013, but an in store vulnerability has again made the data vulnerable to theft. This new ModPOS malware has taken advantage of a flaw in the internal in-store processing of debit and credit transactions still using magnetic stripes as well as using the new EMV Chip and Pin cards; the processing flaw, now known to the retail industry, is that the internal processing systems utilized by many major retailers does not support end-to-end encryption, and does not also properly encrypt data in memory, allowing that credit card data to still be captured and sent to distant cyber crooks. According to iSIGHT, "Criminals can then reuse card data, even from EMV cards, to make online (card-not-present) transactions."

This ModPOS malware can be easily modified to better target specific credit card transaction systems by integrating its own integral data upload and download utilities, "RAM scraping" (capturing unencrypted data in RAM), keyloggers (captures keypad entries, such as PIN numbers), and other highly specialized malware utilities. The malware code itself is encrypted, thus making it very difficult to detect using modern anti-malware detection software and hardware, thus allowing the malware code to burrow itself into the relevant legitimate and necessary computer software, where it is also difficult to detect and neutralize. The malware code was written to not just compromise the retail credit card processing system, but to also install itself in other software used by retailers, rendering it even much more difficult to eradicate. It is important to note that while initially encountered

in retail store payment systems, it has now also been detected in the payment systems utilized in the hospitality industry including some major hotel chains and franchises, and restaurants. It is only a matter of time that ModPOS and similar highly sophisticated malware again appears to threaten our digital transaction systems.

Stay tuned, as we have yet to see if ModPOS and similar malware will in reality wreak havoc on our credit card infrastructure as its malware predecessors did in 2013. While it is still too early to know if, and to what degree, ModPOS and its malware brethren will cost us this season, we should be aware that it is out there, in the wild, targeting our retail and hospitality payment systems. As mentioned in my columns following the infamous massive data breaches of the 2013 holiday season, be absolutely sure to thoroughly check your debit and credit card statements for any questionable activity, and if any suspicious transactions are posted, contact your credit or debit card provider immediately at the phone number on the back of your card.

While in volume and potential financial costs, massive credit card breaches can do extensive damage, there still are some smaller threats appearing in our holiday purchases that many of us would find more irritating than disastrous. It seems that thousands of inexpensive, generic or "no name" Android tablets sold through Amazon and other reputable dealers, were manufactured with malware installed on the devices at the time and place of manufacture in China. There have even been some published reports that some models of major name brand Android tablets, possibly produced by the same makers that produced the infected generic tablets, were also factory infected with malware. According to a November 16 posting by Jeff Goldman on eSecurityPlanet (esecurityplanet.com/mobile-security/android-tablets-sold-on-amazon-infected-with-cloudsota-trojan.html), "Android Tablets Sold

on Amazon Infected with Cloudsota Trojan; The tablets have been sold and delivered to over 17,000 customers in more than 150 countries." Citing a post on the Cheetah Mobile security blog which said, "Researchers at Cheetah Mobile recently found a Trojan called Cloudsota pre-installed on some Android tablets that were available for sale on Amazon.com and other online stores. The Cloudsota Trojan enables remote control of the infected devices, and it conducts malicious activities without user consent," Over 30 brands of inexpensive Android tablets sold by Amazon and other online retailers were infected with this trojan. The top selling brands, which included the vast majority of the infected tablets were "No Name" (unbranded); AllWinner; Soft-Winners; Advance; Rockchip; Joinet; SW; WonderMedia; RDA; Freeman; WorryFree; MID-1013D; ELVISION; and Killer. There have also been published reports of the Cloudsota Trojan being factory installed on some inexpensive, generic branded Android powered smart phones, according to Cheetah Mobile.

The Cloudsota Trojan is a revenue generating type of malware that loads advertising and other apps to the device without the users' permission, and connects as often as every 30 minutes to a web server in China for instructions, updates, and for new apps to be transparently installed without the consent of the users. This trojan also redirects web traffic to its own browser, often blocking the browser selected by the user. Other nefarious activities of this trojan include changing the boot animation of the device to an advertisement; the uninstallation of apps installed by the user, notably antivirus and other security apps; resets the wallpaper to paid advertisements, often showing new advertising every time the "home" button is tapped; loads and runs apps on its own, even if not selected by the user; and displays popup advertisements at random times, regardless of what is being run at that time.

Reputable sellers of these 17000 infected tablets are aware of the problems, and some have offered adjustments or replacements to buyers. For owners of these trojan infected tablets, Cheetah Mobile has published "Manual removal instructions of CloudSota", available online at cmcm.com/article/share/2015-11-09/840.html. The manual removal instructions require the user to connect the tablet to a PC with a common USB cable (often the same cable used to charge most Android phones). The online instructions direct the user to download a file (free) "android-tools.zip" to the PC from Cheetah Mobile, and then follow the online instructions to permanently remove the trojan.

It is shameful that malware authors will commit criminal acts to enrich themselves by stealing our credit card data or infecting smart devices at the time of manufacture with revenue generating trojans. As stated above and in earlier columns, it is imperative that we all routinely check our credit and debit card statements for questionable transactions, and report them immediately to the card companies. While not as perilous, but extremely annoying, thousands of people receiving inexpensive Android tablets this holiday season will be in possession of devices loaded at the factory with malware. Again, contact the seller for replacement or refund, or follow the instructions above for removal of the malware, but also be aware that many of the generic manufacturers of these inexpensive tablets offer no technical support.

It is sad that what should otherwise be a happy time of year turns out to be a less than happy season, all due to the greed of unscrupulous individuals. Pity.

This article was reprinted with permission of the author, Ira Wilsker.



How To Stream TV

by Sandy Berger, CompuKiss

Sandy@compukiss.com www.compukiss.com

There is no doubt that the world of television content and the way we get that content is changing. Many people are “cutting the cord” by turning their backs on cable and satellite TV. These folks are turning to streaming TV shows and movies. For those of you who are not yet familiar with “streaming”, here’s a quick tutorial on how to stream and what you need.

Streaming is named for a technique for transmitting data over the Internet so that it can be processed as a steady and continuous stream. This differs from downloading content in which the entire chunk of data must be downloaded before it can be processed. Most users do not have enough bandwidth to download an entire movie or TV show, so streaming is a great technique. During streaming the content is constantly being processed so you can watch the show while it is being processed with no interruption.

Streaming allows you to watch television shows and movies without having a cable or satellite subscription. You can use streaming to augment a basic cable or satellite TV subscription or to eliminate cable or satellite subscriptions completely making it a valuable tool for TV watching.

Also, Netflix and Amazon are now producing their own programming, much of which, like House of Cards, has become very popular. With streaming you can also watch a wide variety of movies and the past episodes of many different TV shows.

Even if you are not technically inclined, you will find that streaming is quite simple to setup. Here’s what you need.

First -- an HDTV with an HDMI port. While older analog TVs can also be

set up to stream, having an HDMI port makes it much easier. All HDTVs, which include most newer TVs, have these ports. To find them look at the back of the TV. They are usually labeled HDMI.

Second – You need a good broadband Internet connection. This is how the data (movies) will get to your television. The faster the better and you might want to upgrade your Internet, but you may not have to. Try it with the connection you have right now. You might be pleasantly surprised.

Third -- you need a streaming media device. Some newer TVs and most Blu-ray players can access the Internet. If you have one of these you can use it as your media streaming device.

If you don’t have one of these, you will need to purchase a new device. The good news is that these devices are small and inexpensive. These devices include Chromecast, Roku, and Amazon Fire TV and Fire Stick. They range in price from \$30 to \$100. I have tried them all and they all work quite well. If you already belong to Amazon Prime, an Amazon Fire might be the best choice. To get the best selection of content, Roku is the best. In any case, the main difference in price is often whether the device comes with a remote control or not. If it doesn’t come with a remote, like the Chromecast, you will have to use a tablet or mobile phone to control it. If that doesn’t appeal to you, opt for one with a remote.

Fourth -- you will need a wireless router. Although some devices can hook up directly to your wired Internet router, in most cases your television is not in the same room as the Internet connection, making it necessary to have a wireless router to transmit the data wirelessly to your televi-

sion. If you already have wireless in your home for a tablet or phone, you are all set.

When you get your streaming media device home, you simply plug it into the TV. Set the TV to the proper input like HDMI 1 or HDMI 2, then follow the set up instructions that will appear on the screen. All are easy to follow. The only thing you will need is to know the password for your wireless network if it is password protected.

After the setup you will see your choices of things to watch. Some of these will be free, some will have extra costs. For instance Netflix and Hulu both have a ton of content, but each charges about \$10 a month. Fortunately both have free trials which you can use.

Watching streaming media on your TV is not as simple as watching cable TV. There are little inconveniences. Every time you want to switch to your streaming device, you have to change the input on your television. Also there is no simple guide as the one you get with cable or satellite TV. You often have to search for what you want to watch. The Amazon Fire TV (not the Fire Stick) makes this easier because its remote has a voice search which works quite well. Just speak the name of a movie, actor, or director and it will find the movie you want. This, however, only works for Amazon Prime movies and shows. Also, if you have more than one subscription, you have to remember which movies are on which service....Now was “Orange is the New Black” on Netflix, Hulu, or Amazon?

Yet, the inconveniences are minor and there are advantages. For instance, after I started streaming I was able to watch the entire series of “Downton Abbey” on Amazon and “House of Cards” on Netflix at my convenience. How wonderful to watch a few episodes a week until I got caught up!

If you haven't yet tried streaming, be sure to check it out. You may find a new way of watching television that can save you money and give you new options.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.



Microsoft Upgrading Windows 10 - May "Automatically" Upgrade Windows 7 and 8.1 to Windows 10

by Ira Wilsker

WEBSITES:

<http://www.techrepublic.com/article/massive-windows-10-update-could-turbo-charge-windows-7-machines-says-microsoft/>

<http://windows.microsoft.com/en-us/windows-10/upgrade-to-windows-10-faq>

<http://www.techrepublic.com/article/five-ways-microsoft-plans-to-get-you-to-upgrade-to-windows-10/>

www.zdnet.com/article/windows-10-growth-sluggish-as-windows-7-windows-8-users-stick-with-their-os/

<http://www.zdnet.com/article/my-biggest-problem-with-windows-10-stability/>

<https://netmarketshare.com>

<http://www.zdnet.com/article/microsofts-big-windows-10-goal-one-billion-or-bust/>

<http://gs.statcounter.com/#desktop-os-ww-monthly-201508-201510-bar>

<http://www.zdnet.com/article/dont-let-the-grinches-put-you-off-windows-10/>

Several months ago, Microsoft offered millions of users of Windows 7 and 8.1 a free online update to the then newly released Windows 10. While Microsoft has claimed that as many as 110 million Windows 7 and 8.1 users did accept the free offer to upgrade to Windows

10, Microsoft has also expressed some concern that as many as a billion other Windows 7 and 8.1 users have not yet upgraded to Windows 10. According to several published reports, Microsoft has expressed concerns that the rate of Windows users upgrading from the older versions of Windows to Windows 10 has slowed, and this decline in the rate of people upgrading to Windows 10 may cost Microsoft substantial potential revenues.

According to an article published on ZDnet in November (zdnet.com/article/windows-10-growth-sluggish-as-windows-7-windows-8-users-stick-with-their-os), the results of upgrades to Windows 10 during the month of October had slowed compared to previous months. Despite heavy promotions and the springtime appearance of the "Get Windows 10" icon in the system tray of countless Windows computers running Windows 7 or 8.1, the rate of increase in Windows 10 usage has slowed. In October (2015), the number of PCs running Windows 10 was a paltry 7.94%, up 1.31% from the 6.63% rate tallied the month before (September). In September the rate of Windows 10 upgrades was 1.42%, slighter greater than the following month of October, documenting that the rate of increase of Windows 10 upgrades has been slowing. Microsoft has not been as successful as they had hoped in getting people to upgrade their PCs from earlier versions of Windows to Windows 10, as the proportion of desktop PCs running Windows 7 in October was well over

half at 55.71%. In the first week of December, 2015, according to the website NetMarketShare.com, considering the early holiday sales of PCs, the rate of desktop PCs running Windows 7 increased slightly to 56.11%, and the number of PCs running Windows 10 was up to 9%, but this 9% number includes both PCs upgraded from earlier versions of Windows as well as the sales of new PCs with Windows 10 factory installed. Despite the lamentations expressed by many of the users of Windows 8.1 about the foibles of that operating system, Windows 8.1 users have apparently not flocked to Windows 10 to the degree that Microsoft has apparently wanted. According to the article on ZDnet, referencing the October figures, "Windows 8 and 8.1 users just aren't migrating at all (cumulative the usage share for this OS is at 13.22 percent, down only 0.10 of a percentage point)."

Despite the pronounced efforts of Microsoft to get users of Windows 7 and 8.1 to take advantage of the free upgrade to Windows 10, there is still significant resistance in the PC community to the upgrade. While some users of earlier versions of Windows are inherently resistant to change, being relatively happy with the current functionality and performance of Windows 7 on their computers. ZDnet and other online publications have expressed mixed results with PCs upgraded from Windows 7 or 8 to Windows 10, an attitude common among individual users who have performed the upgrade. It is also useful to note that an unknown but probably sizeable number of users who did indeed download the Windows 10 upgrade who went on to perform the upgrade decided to go back to Windows 7 or 8 taking advantage of a little known feature of the Windows 10 upgrade process that allows users to roll back their Windows 10 upgrade to their earlier operating system, and option only available to upgraders for a finite number of days, typically 31 days, after the upgrade. The rollback can be

accomplished by clicking on the Start button, then Settings, "Update and Security", and finally "Recovery and Uninstall Windows 10". If all works as it should, the PC should be restored to its prior operating system.

Earlier this fall, in September, ZDnet published an item, "My biggest problem with Windows 10: Instability", by Mary Jo Foley (zdnet.com/article/my-biggest-problem-with-windows-10-stability). In this article, Ms. Foley summarized her Windows 10 experience as, "Windows 10's strength -- its comprehensiveness -- is also its biggest weakness. Too many moving parts are making for an unstable computing experience for me." While many users were delighted with Windows 10 after their upgrade, this article reflects the results and frustrations that many individual users experienced following the upgrade to Windows 10.

Microsoft has been well aware of the concerns expressed by many Windows 7 and 8 users over such factors as boot time, privacy, reliability, speed, complexity, and other issues which discouraged users from upgrading to Windows 10 (zdnet.com/article/dont-let-the-grinches-put-you-off-windows-10). To help overcome these objections by millions of users who have not taken advantage of the free upgrade to Windows 10, as well as to address issues of performance and other concerns of Windows 10 users, Microsoft recently released a major upgrade to Windows 10. In a recent article in TechRepublic, dated November 12, and written by Nick Heath, "Massive Windows 10 update could turbo charge Windows 7 machines says Microsoft. The first major update to Windows 10 hits today - with Microsoft promising great things for those upgrading from Windows 7,

as well as significant new features for business users." (techrepublic.com/article/massive-windows-10-update-could-turbo-charge-windows-7-machines-says-microsoft).

This new update to Windows 10 is a huge download of slightly less than 4GB, and is claimed by Microsoft to speed up the PCs' boot time by up to 30%, making Windows 10 boot faster than the Windows 7 which had previously been running on the same machine. According to Jeremy Korst, general manager of the Windows and Devices team at Microsoft, "There's a bunch of things under the hood that we've improved with this update to make it an even better experience." Microsoft has indicated a desire that the improved features, performance, compatibility, and stability of the upgraded Windows 10 will help convince Windows users who have not yet upgraded to Windows 10. Microsoft has planned some strong encouragement for those users, because in early 2016, Microsoft will start to "push" the upgrades of Windows 10 to PCs still running Windows 7 and 8.1.

Starting in 2016 (the exact official date has not yet been published, but a variety of commencement dates have been suggested), Windows 7 and 8.1 will automatically begin installing the

upgraded Windows 10 after a user confirmation during the conventional Windows update process. According to Jeremy Korst, "(T)he customer will have the ability to delay it for some period", that "period" being unspecified. As with the previous, more voluntary upgrades, the user may be able to restore his prior operating system within 31 days of installing the free upgrade to Windows 10. Jeremy Korst continued, "We'll be taking customer feedback throughout this process and the intent really is to make the upgrade even easier for customers." This corroborates an earlier article (October 30) by Nick Heath in TechRepublic (techrepublic.com/article/five-ways-microsoft-plans-to-get-you-to-upgrade-to-windows-10). This article, "Five ways Microsoft plans to get you to upgrade to Windows 10" explains that Microsoft, "(In order) To achieve its goal of getting one billion people onto Windows 10, Microsoft is getting more forceful in how it pushes Windows 7 and 8.1 users towards its new OS." Primarily this will occur when Windows 10 automatically begins installing itself as a "Recommended Update", which means that the majority of Windows users who have the default "Install Updates Automatically" setting will transparently have Windows 10 installed. Microsoft has stated that us-



ers will need to confirm the installation before it begins, but it is well known that most users blindly "OK" Microsoft's recommendations. Being aware that many internet users have metered or limited access, Terry Myerson, Microsoft's executive VP of the Windows and Devices Group, says that "(Users) have the option of turning off automatic updates" but does not recommend that they do turn off automatic updates due to, "... the constant risk of internet threats". Microsoft will also make it easier for those who want to initiate the upgrade to Windows 10, rather than wait for the updates that will be pushed to them; the "Get Windows 10" icon in the system tray will soon get an "Upgrade Now" option, which will immediately start to download the huge upgrade file, and commence the upgrade process. For those who may have multiple PCs which they would like upgraded to Windows 10, will shortly find that the process has been made much easier. Microsoft has released its "Media Creation Tool" which can create an image file that can be installed to a

USB flash drive or a DVD disc, and then used to upgrade multiple machines without having to download the huge file to each of the PCs. This "new and improved" single image file will be able to upgrade PCs to an appropriate flavor of Windows 10, including 32 and 64 bit versions, as well as the Home or Professional versions of Windows 10, all from that single image file. This image file can also be used for a "clean install" of Windows 10 provided the user has a valid Windows license.

The new year 2016 will be an interesting one for Windows PC users still using Windows 7 or 8.1. I expect some users to be happy with the new, somewhat "forced" upgrades to Windows 10, while many others to complain loudly. Happy new year, Windows users.

This article was reprinted with permission of the author, Ira Wilsker.



Presenters Wanted

The officers invite any member to make a presentation at the main meeting.

If there is some software you have been using and think others may be interested as well, or there is a computer topic you would like to present to other members, please call or e-mail Don VanSyckel. Making presentations is not that difficult. The hour goes by before you know it and there is always enough material to cover in a software package so that the hour is easy to fill.

If there is a topic you are interested in or something you would like demonstrated, please see any of the officers. They are always interested in what the members would like to see.



If your e-mail or mail address changes, please e-mail: secretary@SterlingHeightsComputerClub.org

Where To Get Instructions For Your New Devices

by Sandy Berger, CompuKISS
www.compuKISS.com sberger (at) compuKISS.com

If you are ready to learn a little more about your cell phone or tablet to make the most of your investment, you may find it difficult to find the instructions you need. This is especially true because none of the today's devices come with any sort of instruction manual. That means that you have to find your own way of getting the information you need.

The best way to do that is to visit the manufacturer's website and find the support area.

Apple manuals and user guides at <https://www.apple.com/support/iphone>

Windows devices, search the Microsoft website

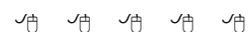
Android devices, go straight to the manufacturer

- For instance, if you just got a Samsung Galaxy S5, the manuals are at www.galaxy5manuals.com
- Smartphones, you can also check out the website of your service provider
- For instance, Verizon has tons of information including videos on using the Galaxy S5 on their website at www.verizonwireless.com/support/galaxy-s-5



SHCC Emergency Cancellation

Sterling Heights Computer Club meets at Macomb Community College (MCC). We will meet if MCC is open and will not if MCC is closed. MCC closure is announced with other school closings on many local TV and radio stations and on their web site. All members of SHCC have an email address. One of the SHCC officers will send an email to the addresses SHCC has on file alerting members to the event cancellation. If your email is broken, call an officer; don't leave a message, call another officer if you don't talk to someone live. It is your responsibility to keep the email address you have listed with SHCC current.



WYSIWYG WEB WATCH (www)

by Paul Baecker webwatch@sterlingheightscomputerclub.org



This column attempts to locate sites containing valuable, amusing and free content, with no overbearing pressure to purchase anything. Send your favorite entertaining, helpful or just plain useless sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG.

35 ways to declutter in 51 seconds. Oh-oh, this is really going to hurt!

<http://www.msn.com/en-us/video/homechannel/35-ways-to-declutter-in-51-seconds/vi-BB9drO4?ocid=mailsignout>

Collection of 16 'best free PC games'. Some require the free Steam Entertainment Platform installed (for Windows, Mac, and Linux).

<http://www.pcworld.com/article/2457868/software-games/the-17-best-free-pc-games.html#slide1>

Gaping security hole in many Dell computers. Be sure yours is patched.

<https://davescomputertips.com/dell-pcs-ship-with-huge-security-hole-a-la-superfish/>

How to update the firmware of any device in 5 steps.

<http://www.digitalcitizen.life/how-update-firmware-any-device-6-steps?>

<http://www.digitalcitizen.life/how-update-firmware-any-device-6-steps>

New Ransomware steals passwords.

<http://techtalk.pcpitstop.com/2015/12/09/new-ransomware-steals-passwords/?ransomware-passwords=>

If you regularly use Google services, then you will definitely want to know what it knows about you, to customize or delete information.

<https://www.maketecheasier.com/what-google-knows-about-you/?maketecheasier-googleknows=>

How to turn off telemetry in Windows 7, 8, and 10.

<http://windowsitpro.com/windows-10/how-turn-telemetry-windows-7-8-and-windows-10>

How does Twitter work anyway?

<http://momthisishowtwitterworks.com/>

How does Twitter work anyway?

<http://momthisishowtwitterworks.com/>

Fixing some common Facebook issues.

<https://davescomputertips.com/fixing-common-facebook-issues/>

Every pet needs an iPad.

<https://www.youtube.com/watch?v=KXgHMgqGlwE>

<https://www.youtube.com/watch?v=la6vK6hI7rM>

How to fix Windows 10's worst problems. (2 parts)

<http://betanews.com/2015/08/12/how-to-fix-windows-10s-worst-problems/>

<http://betanews.com/2015/10/23/how-to-fix-windows-10s-worst-problems-part-2/>

Download Windows 10 with the November (2015) Update and create your own installation media.

<http://betanews.com/2015/11/12/how-to-download-windows-10-with-the-november-update-and-create-your-own-installation-media/>

4 ways to protect yourself against keyloggers.

<http://www.makeuseof.com/tag/4-ways-protect-keyloggers/>

7 things to do after installing Ubuntu.

http://www.itworld.com/article/2997550/linux/7-things-to-do-after-installing-ubuntu.html?phint=newt%3Ditworld_today&phint=idg_eid%3D5392a04cd05d830a67aa8eee99738298#tk.ITWNLE_nlt_best_2015-10-29

11 hidden tips and tweaks for Windows 10.

<http://www.itworld.com/article/2995056/windows/11-hidden-tips-and-tweaks-for-windows-10.html>



NOTE: Many of the links in the digital newsletter connect to the Internet if clicked. For those that do not, copy the link into your browser, and reach the web site that way.

World Wide Web Column on the Club Web Site

Check out the WebPageReviews section on the club's web site. You can see past web sites reviewed in this column on our club web page. They are arranged into various key word categories to help locate a specific site.

