Midland Computer Club

Midland Michigan

BITS AND BYTES

April 2015

http://mcc.apcug.org/

President Piper's Ponderings....

All the Board members at our April meeting were able to connect their tablet, phone or laptop to our new Epson projector. We will give a brief demonstration at our April General Meeting on how to make the connection, as well as hand out a one page sheet that explains the process. If you want to try to connect your tablet, download the Epson iProjector free app, and you can try at the end of our meeting.

The topic for April will focus on recovery and diagnostic CDs; a related article is in the April Bits and Bytes (page 3). One of these CDs might save you big bucks at a repair shop.

If there is time, I also want to talk about the website ninite.com. It is a slick and easy way to install up to 87 basic programs on a PC. It requires very little time on your part, and you avoid any "crapware" that often comes with free programs. It will sound too good to be true when you hear about it, so check out the website before our April meeting to help you make up your mind.

There is a rumor that only one Club member is still running Win XP. The Board talked about having another meeting on Win 8.1 and Win 10, but that probably won't happen until the fall.

I hope to once again try to record a meeting. I still have a good, operational inkjet printer to give away. I just need to make the effort to bring it to a meeting.

See you Wednesday, April 22 at our General Meeting

(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)

GENERAL CLUB MEETING

Midland Community Center, 2001 George St., Midland MI
Room K111, Barstow Shipps Wing

Wednesday, April 22, 2015
7:00 P.M.
Topic: When All Else Fails - Larry Piper
Diagnostic and Bootable CD's

2015 BOARD MEMBERS

MCC OFFICERS

President	Larry Piper	larryp56@chartermi.net
Treasurer	Jan Ensing	btiger6@yahoo.com
Membership	Gary Ensing	btiger6@gmail.com
Editor & Webmaster	Carol Picard	webbyte@yahoo.com

AT-LARGE BOARD MEMBER

Joe Lykowski joseph@lykowski.com

PROGRAM COORDINATORS

Howard Lewis lewis3ha@chartermi.net
Bill Tower tower.w@gmail.com
Please let Howard or Bill know of topics you would like covered at future meetings.

PUBLICITY

Al Adams aladams12@yahoo.com

Board Meeting

First Thursday of the month
7:00 PM
Chapel Lane Presbyterian Church,
5501 Jefferson Ave., Midland MI

Useful, useless and strange (in no particular order) Web Sites:

http://www.houseboating.org/
Spend your next vacation on the water by renting a houseboat on one of over 30 lakes across the U.S.

http://forums.anandtech.com/
If you are having technical problems, the forums on this sight might be able to help. You can search the many different technical articles, but if you want to post a question, you will have to register first.

https://archive.org/details/internetarcade
This site hosts many different video arcade games from the 1970s to the 1990s that can be played in your browser.

http://www.storyoftheweb.org.uk/
This site documents the history of the web as we know it from 1989 to today.

http://tinyurl.com/p724yhu
Watch this dog play pool!

Membership Enrollment Form

NAME _____ *PHONE* _____

ADDRESS _____

CITY _____ *ZIP* _____

EMAIL ADDRESS _____

Membership dues FAMILY ($20) STUDENT ($15) New Member ____ Renewal ____

Please fill out the above form and mail it along with payment of check or money order to :

MIDLAND COMPUTER CLUB
1816 Bauss Ct
Midland, MI 48642-4023

Attn: Membership Chairman

You may also pay for membership at a regular club meeting

Tips, Tricks & Techniques

When all else fails …

You're faced with a sick PC that, for some reason, will not allow your normal antivirus and malware removal software to function. You may not be able to boot the PC, or if you can, the PC doesn't respond to anything you try. You may have even removed the HD and tried to clean it by connecting it to another PC. You're beginning to think reformat, reload the OS and then reinstall all the software. If you are lucky, you may have been able to copy your data while the HD was connected to a second PC.

But there is another alternative—boot the sick PC with a "special" CD which then runs an antivirus program. I had the "opportunity" to learn about this technique when three events simultaneously occurred in my life: 1 – I had agreed to fix a sick PC for a "friend", 2 – I was so sick with a cough that I couldn't do anything except sit in front of my PC for a couple weeks, and 3 – I ran across an Internet article titled *15 Free Bootable Antivirus Tools*. (http://pcsupport.about.com/od/system-security/tp/free-bootable-antivirus-software.htm)

The technique is simple, but time consuming. You download an ISO file, burn it to a CD, boot the sick PC with this CD, watch it update its database from the Internet, then wait for a couple hours while viruses are removed from the sick PC. As the article suggests, there are 15 different CDs you can try. I created 12 of the boot CDs, and I ran 10 of them on the same sick PC. I couldn't get 2 of them to work. My results, below, are based in order upon how good a job each did, how easy it was to run and how long it took to run.

I liked Avira, DrWeb, AVG, Windows Defender, Kapersky, Anvisoft, Bit Defender, Comodo, Zillya and F-Secure. I did not try Alt OS, VBA32 and Sophos. The two I could not get to work were Trend Micro and Panda. That's too bad, because I would have thought those two should have been some of the best.

If you are still with me, I next uncovered an article titled *5 Free Bootable Diagnostic Tools. (http://lifehacker.com/5551188/best-computer-diagnostic-tools) These include: Hirens, Ultimate Boot CD, SIW Portable and BartPE. The author's fifth tool was Google search. I tend to try Google first when I have a problem, but many people responded to this article by saying that Google was not a tool. Each of the above four CDs contain a myriad of programs that aid not only in repairing a PC, but also in revealing the details of your hardware and software. One could spend a couple weeks trying all the options on these 4 CDs.*

Finally, I uncovered a third article titled *5 Free Rescue Discs. (http://www.gfi.com/blog/top-5-free-rescue-discs-for-your-sys-admin-toolkit/) Besides Hirens and Ultimate, from the above article, this article also included Falcon4, System Rescue and Trinity Rescue. Again, these discs have a lot of firepower that will come in handy when you have problems. For example, the Trinity CD told me my laptop was running hot. I opened it up, cleaned out the fuzz from around the fan, and now it works fine.*

Happy Trails,

Larry Piper

ARTICLE INDEX

Decrypt Instructions or I've been infected with Cryptowall, now what? -- Page 4
Frank Ramsey, Newsletter Editor, Akron Canton PCUG, Ohio
Windows 8.1 - Downloading, Purchasing and Installing Apps -- Page 9
Rosita Herrick, Director, Sarasota Technology User Group, FL
Interesting Internet Finds -- Page 11
Steve Costello, President / Editor, Boca Raton Computer Society, FL
Windows 8.1, iOS7 and Other Updates -- Page 12
Sandy Berger, Compu-KISS
Are You Safe from a Cyber Attack? -- Page 14
Lou Torraca, President, The TUG-MOAA User Group, Hawaii
APCUG's FREE 2015 Spring Virtual Technology Conference (VTC) -- Page 16

Decrypt Instructions or I've been infected with Cryptowall, now what?

By Frank Ramsey, Newsletter Editor, Akron Canton PCUG, Ohio
www.acpcug.org, aframsey (at) yahoo.com

Have you ever booted your computer only to have the following displayed?

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0
.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed; you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http://paytordmbdekmizq.tanktor.com/sRkkc
2.http://paytordmbdekmizq.bladetor.com/sRkkc
3.http://paytordmbdekmizq.batmantor.com/sRkkc
4.http://paytordmbdekmizq.torbama.com/sRkkc

If for some reasons the addresses are not available, follow these steps:

1.Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2.After a successful installation, run the browser and wait for initialization.
3.Type in the address bar: paytordmbdekmizq.onion/sRkkc
4.Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal page: http://paytordmbdekmizq.tanktor.com/sRkkc
Your personal page (using TOR): paytordmbdekmizq.onion/sRkkc
Your personal identification number (if you open the site (or TOR 's) directly): sRkkc
---

I certainly hope not! Because if this happens, you've been infected with ransom ware Cryptowall!

What is Cryptowall?

It's a complex piece of malware that copies files from your computer to a server on the Internet, then encrypts the files on your computer using a public/private key combination. The last thing it does is cleanup after itself, trying to remove any copies extra of the files found in places like the Recycle Bin. Then it places a file with the decrypt instructions in text and html in every directory containing encrypted files.

More details on Cryptowall can be found at http://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information

Should I believe what it says?

YES! Your files have been encrypted and there is no way to decrypt them without the private key. Getting the private key requires you to pay the ransom. Your only hope is to rely on backups or try to recover the files from the Recycle Bin or shadow copies.

What files does it attack?

The files encrypted are the ones you typically the most important to you, including Word documents, Excel spreadsheets, PowerPoint presentations, pictures and videos on both local and network drives. Yep, you read this correct. If it's got a drive letter, Cryptowall goes after it.

What can you do?

What you do depends on how important the encrypted files are to you. The file types the ransom ware encrypts are typically Office documents, pictures, videos, etc. If you don't have a backup of these in a location not accessible to Cryptowall, you might consider following the instructions listed.

1) Pay the fee
If you follow the instructions, you are guided to the private key to be used to decrypt your files and a decryption application after payment. The payment is only in Bitcoins. These are basically untraceable.

The instructions have you use a torrent browser, which is also basically untraceable.

The cost starts at $500. If you don't respond in 7 days, the price increases to $1,000. In Bitcoins of course.

Recover the lost files

If you've practiced good backups, you should have copies of the files available for restoring. Your only decision is to try and clean up the ransom ware before restoring the files or start from scratch by reformatting the hard drive and reinstalling all the applications from scratch.

Let's say you're like most of us and don't have backups, then you are forced to see if the cleanup phase of Cryptowall intended to delete copies of the files actually deleted the copies.

Check the Recycle Bin. You're probably not going to find clean copies of the files, but it's worth a shot.

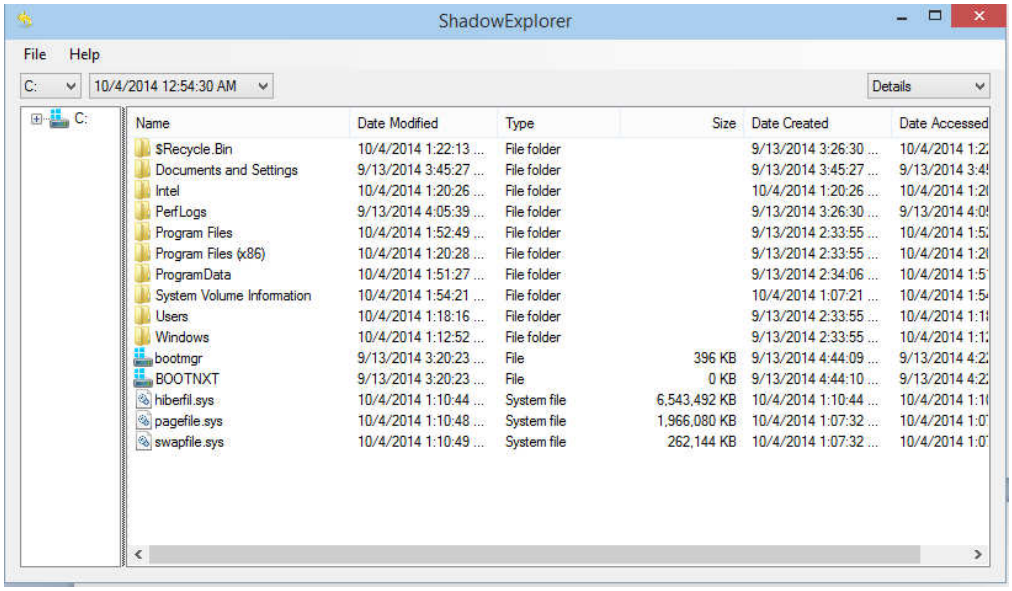
Another thing to try is a System Restore. Originally designed by Microsoft to recover critical system files, it has been enhanced to recover user files. My experience with System Restores is hit and misses. It may work, it may not. Each try takes time.

The last option is to check Shadow Volumes. "If you had System Restore enabled on the computer, Windows creates shadow copy snapshots that contain copies of your files from that point of time when the system restore snapshot was created. These snapshots may allow us to restore a previous version of our files from before they had been encrypted. This method is not fool proof, though; as even though these files may not be encrypted they also may not be the latest version of the file. Please note that Shadow Volume Copies are only available with Windows XP Service Pack 2, Windows Vista, Windows 7, & Windows 8." (from bleepingcomputer.com).

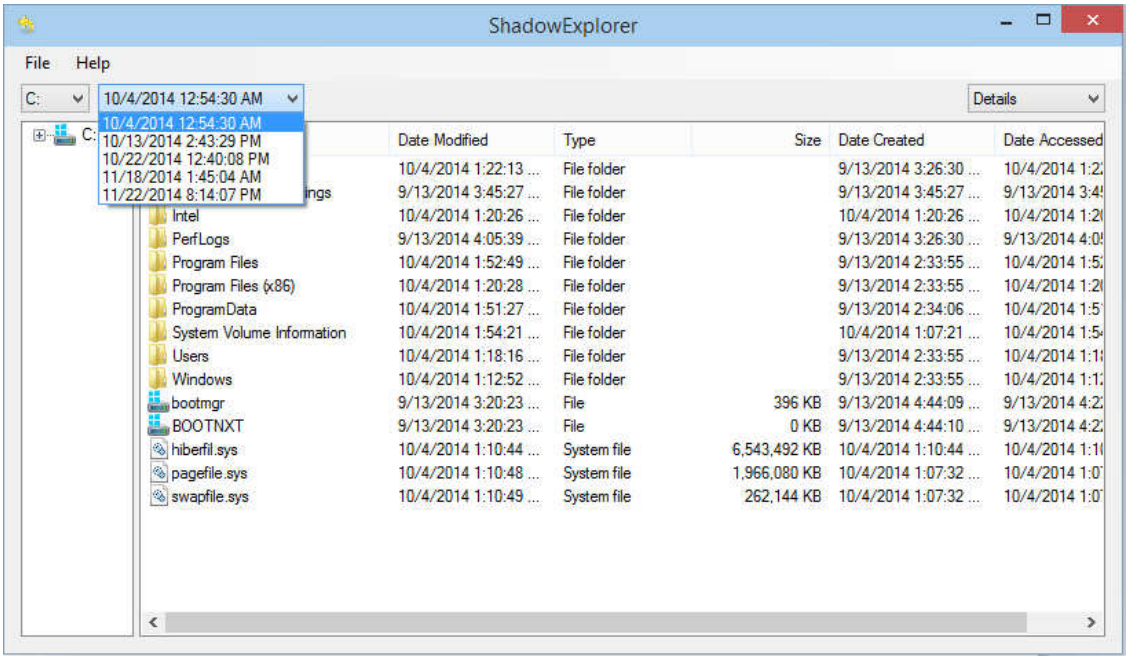
As bleepingcomputer.com says Shadow Volumes may or may not be available. You can check file properties, the previous version tab to see if any are listed.

Or you can get ShadowExplorer from Shadowexplorer.com. It's free. I suggest the portable version. Download the zip file, expand it, then run Shadowexplorerportable.

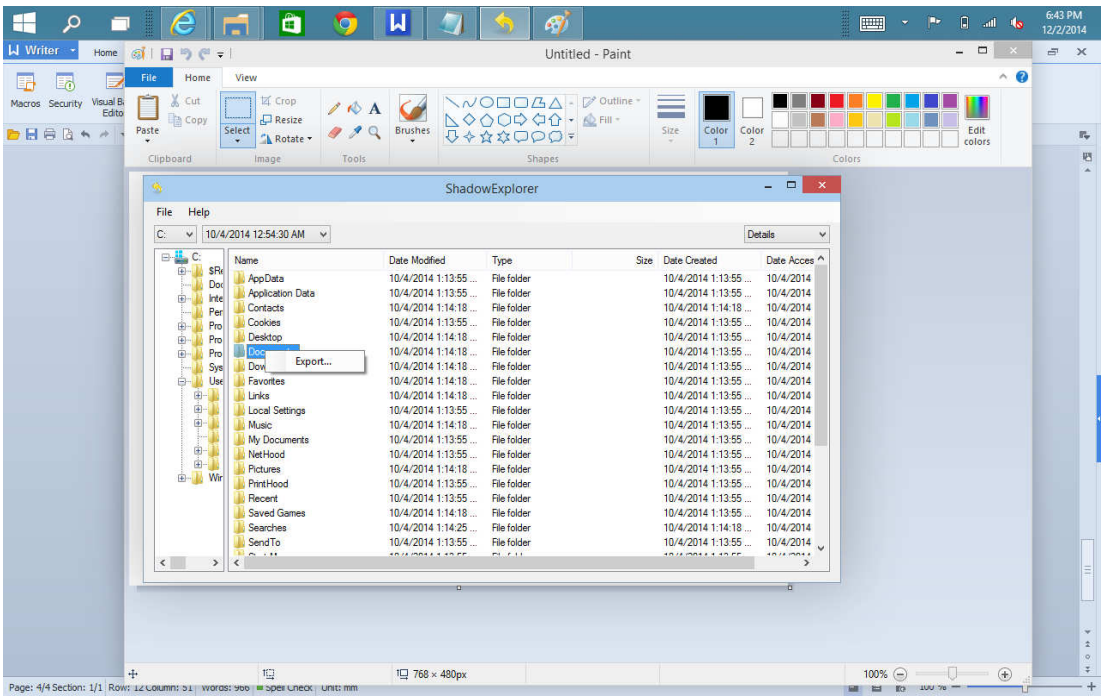
The main screen is displayed



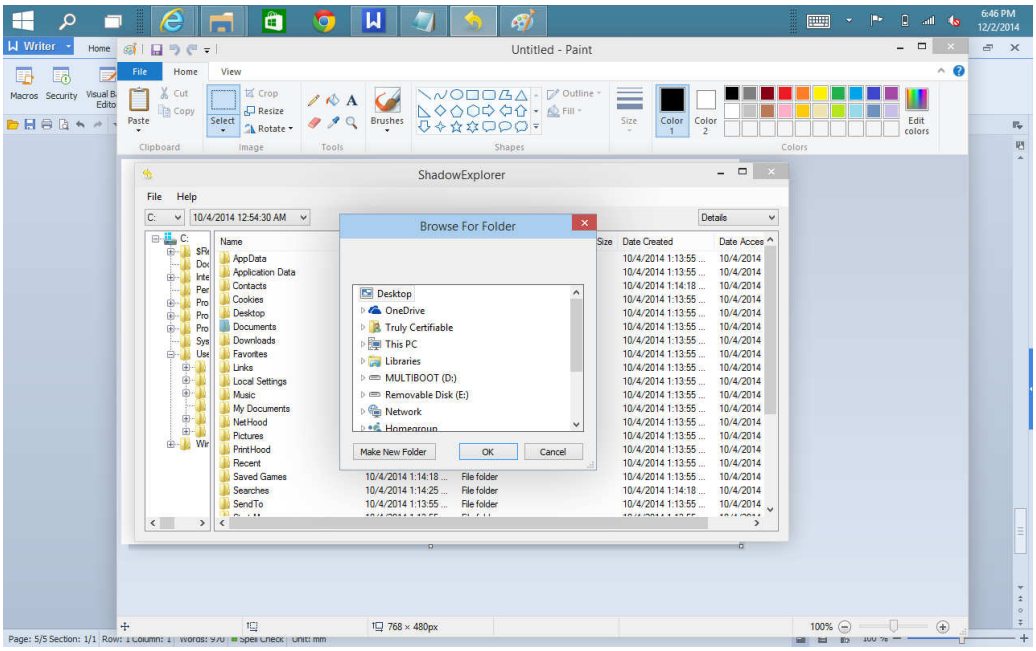
If you select the drop down box you can see the Shadow copes that are available.



Select the Shadow copy before the ransom ware was run, browse to the files you would like to recover, then right click and select export.



Then select a location to save the export and click OK.



Once it's done, you're back to same decision as in the step above. Should you try to clean up the ransom ware and copy the files back or reformat the hard drive and reinstall everything from scratch before restoring the files?

Clean up the computer

As mentioned above the decision is try to clean up the ransom ware or reformat the hard drive and reinstall everything from scratch.

My experience (yes, I did have the pleasure of experiencing this first hand) is while this is nasty, it's not self-propagating; i.e. it doesn't continue the infection. It's a one shot deal. Therefore, cleanup is definitely a possibility if you want to take the time.

First search for and delete all copes of DECRYPT_INSTRUCTION* on the hard drive.

Then check and delete the registry entries listed in the bleepingcomputer.com article cited above. That's pretty much it.

I would suggest a full antivirus scan and a complete scan using malwarebytes after the cleanup and before restoring the documents from ShadowExplorer.

What can I do if shadow copies are not an option?

Basically if Shadowexplorer doesn't show any shadow copies, you've got a pretty easy decision. If the files Cryptowall encrypted are worth the ransom, well pay the ransom and get the files back. If the files are not worth the ransom, either cleanup Cryptowall as described above or reformat the hard drive and reinstall everything from scratch.

How can I keep from getting Cryptowall?

First install a quality antivirus. Keep it updated. In my experience, the antivirus was allowed to expire. Hence the system was totally unprotected.

Quality antivirus doesn't mean expensive. The free version of Avast detects and blocks Cryptowall.

Don't open any attachments from people you don't know. This includes pdf's and others. Even those that say you've won the lottery, open the attachment for more details on how to collect your winnings. AVOID THEM!

Windows 8.1 - Downloading, Purchasing and Installing Apps

By Rosita Herrick, Director, Sarasota Technology User Group, FL
www.thestug.org, Rosita (at) spcug.org

In addition to being a computer operating system, Windows 8.1 is blurring the line between the old ways of working on a computer and the access to information used by tablets and smart phones. The distribution of apps that perform individual tasks is one of the ways.

In additions to apps that come with the operating system, Microsoft has created a store for apps distribution.

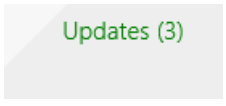
The Store App
The Store app can be found either on the Start screen or on the Task bar.

Access to the Internet is required for accessing the Store.
You access the store app by clicking on the tile/icon.
When the app opens you have quite a few options to search for items of interest.
Once you find an app of interest, just click on it and on the page that opens you will find information about the app such as number of downloads, reviews with rating and a description of the app. The app might be free, might have a price, or it can be downloaded for trial.

Usually a Microsoft account is required. To install the app, just click on the *Install* button.

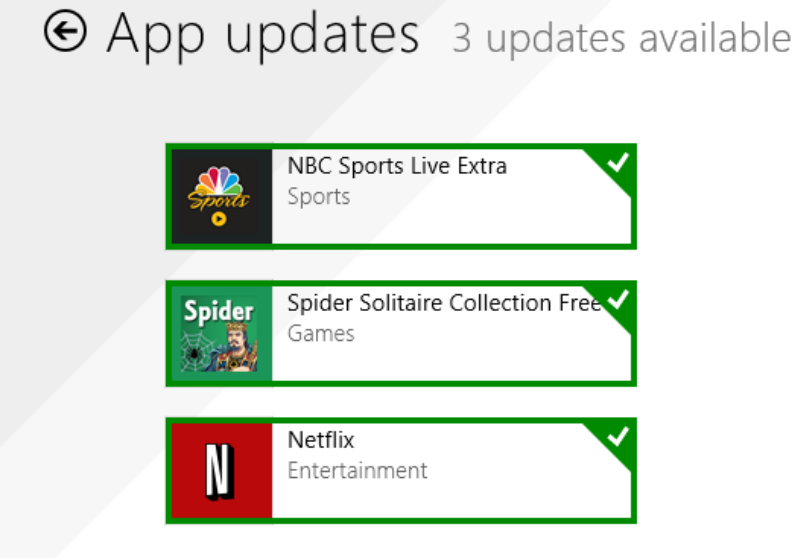
Maintaining Apps
Periodically, there are updates for apps to either enhance them or fix some problem.
To check for updates go to the Store app.

On the upper right side of the screen, if there are updates available for any of the apps, you will see a link in green

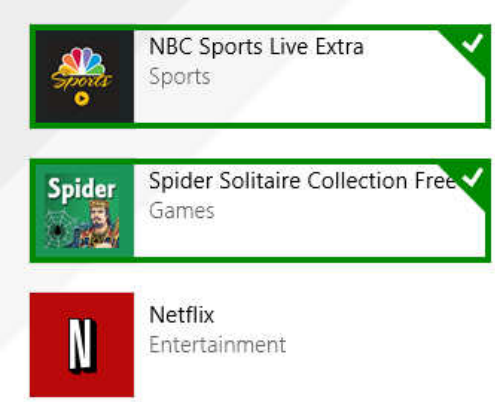


In this case there are updates available for 3 of my installed apps (not distributed with the system).

Clicking on this link displays the 3 apps that are scheduled for an update.

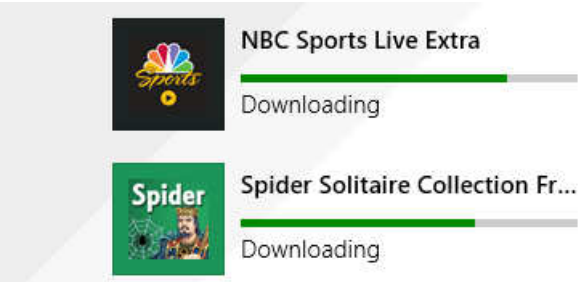


The check mark on the right corner shows that the update is selected to install. It can be unchecked with a right click



Now I can update the two remaining apps by clicking on the install icon at the bottom of the page.

Once I click on install, the following page displays



The amount of time a download and install takes depends on the speed of your internet connection, the size of the update, and the speed of your computer.

Once the download and install are completed the next message on the screen will be:

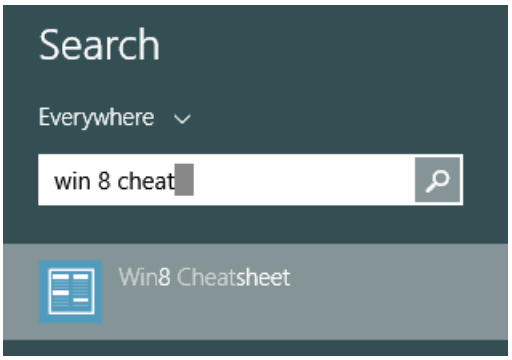
Your apps were installed

You can now close the Store app.

Uninstalling an App

This process is very simple.

Find the app with the search charm.



Right click on the icon and this box will appear.

Click on Uninstall and Windows will remove the app from your system.

Interesting Internet Finds

Steve Costello, President / Editor, Boca Raton Computer Society, FL
editor@brcs.org, http://ctublog.sefcug.com/

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of September 2014.

Is USB safe?
http://askleo.com/is-usb-safe/

Leo Notenboom tells us about the "BadUSB" flaw, what it is and what is known about the implications.

What Does Airplane Mode Do, and Is It Really Necessary?
http://www.howtogeek.com/194421/what-does-airplane-mode-do-and-is-it-really-necessary/

Have a device with airplane mode? HowToGeek explains what it does, and why you should use it, even if you are not on a flight where it is required. I know I use it whenever I don't need to be connected, or when I cannot get any connections, like on my last vacation in Vermont when my wife had service and I didn't.

Beware the Fake Tech Support Scam
http://askbobrankin.com/beware_the_fake_tech_support_scam.html

Bob Rankin talks about the fake tech support scams that are prevalent in different areas and times. He talks about how to recognize them, and avoid them, as well as what might happen if you fall for one of them.

3 Things to Do to Make Your Internet Life More Secure
http://www.maketecheasier.com/make-internet-life-more-secure/

Interested in making you internet life more secure? If so, check out these three things you might not be doing already.

How to set up two-factor authentication on your Google account
http://www.greenbot.com/article/2605221/how-to-set-up-two-factor-authentication-on-your-google-account.html

This post explains how to set up two-factor authentication on your Google account. If you haven't already set it up, you should to keep it more secure.

Online Identity Theft: Prevention and Protection
http://www.thewindowsclub.com/online-identity-theft

The Windows Club explains what online identity theft is, and how to prevent it and protect yourself.

****

Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog: http://ctublog.sefcug.com/tag/interesting-internet-finds/

Windows 8.1, iOS7 and Other Updates

By Sandy Berger, Compu-KISS, www.compukiss.com, sandy (at) compukiss.com

Winston Churchill once said, “To improve is to change; to be perfect is to change often.” It seems that this is the mantra of today’s high tech world. The quest for perfection brings almost constant change. If you use Windows 8 or an Apple mobile device, you will want to read about the changes you need to make.

You get up in the morning and find that your Gmail looks different than it did yesterday. You get an announcement that there is an update to another program that you use every day. Get used to it. Change in the high tech world is inevitable. Most of the time the upgrades and updates bring added security, so you don’t want to stay with the old. You must move on.

This is what many people found with two recent updates. Apple updated their mobile operating system to iOS 7 and Microsoft updated Windows 8 to 8.1. Both of these updates are free for users who owned previous versions. Both add excellent features and increased security. However, both require the users to learn about how to use the new functionality. And, as usual, the user is given no instructions on how to upgrade or how to manage the new programs.

With previous upgrades of Windows, Microsoft performed the update for you if your computer was set to receive automatic updates. Windows 8.1 is different. You must visit the Microsoft Store to initiate the update. Just look for the green Store tile in your Start Screen. Then click on the Windows 8.1 banner in the Store.

Allow at least an hour for the update. When the installation is complete, you will be presented with the familiar color tile Start screen, but there are many subtle differences. First, if you want to search for something, you simply start typing what you want to search for. The search window automatically appears. What is different is that now Windows will search everywhere for you. You no longer have to tell it to search apps, files, etc. Windows will even search the Internet for you and present you with the results in one window.

Another change in Windows 8.1 gives you the ability to boot directly to the Desktop instead of the colorful Windows Start screen. Unfortunately, this option is fairly hidden. To turn it on you will have to go to the Desktop and right-click on the toolbar on the bottom. Choose the Navigation option where you will see the choice to go to the Desktop instead of Start on sign in. You will also see other new choices in this area. They can be turned on and off at will, so feel free to play with them, if you like.

Several apps have also changed with Windows 8.1. One important change is that if you install a new app, it won't automatically show up on the Start screen. You will have to go to the All Apps page, right-click on the app and choose "Pin to Start" to have it show up there.

Apple's new operating system also brings many changes. If you are using a newer iPhone or iPad and you see a small red circle with a number in it above the Settings icon, this is the indication that there is an update available for your operating system. Tap on Settings, then General, then look for the update and give your permission to download and install it.

If this is the update for iOS 7, once complete you will notice that the icons and screens look quite different. This is a good thing since they have improved the clarity of the text and icons. Again, however, there are a few things to learn. In previous versions of iOS, you quit apps by double-clicking the Home button and holding down icons until they jiggled. Now when you double-click Home, you will be presented with all of the running apps as rectangular "cards". To stop an app, just put your finger on the card and flick it off the screen with an upward motion.

The Search on these Apple devices has also changed dramatically. You used to search by moving to the page to the left of the home screen, but that page is gone in iOS7. In order to start a search on your iPhone or iPad with iOS7, put your finger in the middle of the screen and swipe in a downward motion. This will bring up the Search screen and keyboard where you can enter your search terms.

Actually all of these changes are good. Just keep repeating that to yourself as you encounter frustrations at the new way of doing things. Remember change is good and you are on the path to perfection!

Are You Safe from a Cyber Attack?

By Lou Torraca, President, The TUG-MOAA User Group, Hawaii
President@the-TUG.org, www.the-tug.org
Around Hawaii - Oceanic Time Warner Cable's Community Website
http://www.aroundhawaii.com/lifestyle/computers/

I always enjoy reading the “what happened in history” emails I get about once a month, so I was reminded that September had a profound effect on the way we treat our personal technology.

HackerOn September 18, 2001, a new virus attacked United States operating systems. The worm was given the name Nimda, and it was an advanced version of Code Red II. Some might say that the Code Red viruses were created in preparation for the much larger Nimda attack, which was executed the week following the attacks on the World Trade Center and Pentagon. Due to the release date of the virus, members of the American government speculated on a link between the cyber-attacks and Al Qaeda, but this theory ended up proving unfounded. The American media did not report much on the virus because of the terrorist attacks.

Multiple propagation vectors allowed Nimda to become the Internet’s most widespread and dangerous virus. It took only 22 minutes for the worm to rip through the American financial sector, causing over $3 billion in damage. The Nimda virus was so effective because it used five different infection vectors. People could, and still can, get the virus via e-mail, open network shares, infected websites, exploitation, or via back doors left behind by the Code Red II virus. The group of people behind the Nimda virus and the theft of billions of dollars are unknown. The event greatly damaged the world’s financial sector and economy.

There are numerous places you can review various ways to protect yourself, e.g. my last column listed free programs you can download to block viruses and malware. One government agency that has excellent advice is Homeland Security. Here is the page on their website that offers suggestions on how to protect yourself from Cyber Attacks:

What You Need To Know

The Department of Homeland Security plays an important role in countering threats to our cyber network. We aim to secure the federal civilian networks, cyberspace and critical infrastructure that are essential to our lives and work.

DHS’s National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence and law enforcement communities and the private sector.

Next Steps

The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into "clicking the link" or opening attachments to seemingly real websites:

- **Never click on links in emails**. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.

- **Never open the attachments.** Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.

- **Do not give out personal information over the phone or in an email unless completely sure**. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!

Other practical tips to protect yourself from cyber-attacks:

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.
- Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.

Tips

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it.

For example, instead of the password "hoops," use "IITpbb" for "[I] [l]ike [T]o [p] lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "II!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

The website (http://www.dhs.gov) also has links to other pages that have good advice regarding security, as well as other pertinent issues; I suggest you take a look.

That’s it for now, be safe out there. Follow the above advice, but save time to have some fun too.

Aloha, Lou

APCUG's FREE 2015 Spring Virtual Technology Conference (VTC)

will be held on Saturday, May 2, from 1:00 pm – 5:00 pm Eastern Time. The sessions are 50 minutes in length and offer attendees the opportunity to ask questions via a chat window.

Videos from earlier conferences can be found on APCUG's YouTube channel www.youtube.com/apcugvideos.

- Link to register for this VTC: http://bit.ly/APCUG-2015-Spring-VTC

- Link to view the presenter bios, find more information on the presentations, and, after the conference, you can download the handouts and get links to the videos. http://apcug2.org/content/vtc15

TRACK 1

1:00 iPad 101
Jere Minich, APCUG Advisor, Region 5; Program Chair, Lake-Sumter Computer Society

2:00 Picasa, an easy-to-use digital editing program
Wil Wakely, Past President, Seniors Computer Group

3:00 The Good, The Bad, and The Ugly of Recording and Organizing Your Research on the Web
Jeri Steele, President, Bowling Green Area Microcomputer User Group

4:00 Preview of New APCUG WordPress Website
Jim Evans, APCUG Director

TRACK 2

1:00 Selecting the Best Backup Approach
Gene Barlow, User Group Relations

2:00 Are We Under Cyber Attack?
Ira Wilsker, Columnist, Associate Professor, Law Enforcement Officer specializing in cyber crime

3:00 Social Networking: What the Heck are Facebook, Twitter, and LinkedIn???
Abby Stokes, author, A Friendly Guide to Everything Digital for Newbies, Technophobes and the Kicking & Screaming