QBITS

Quad-Cities Computer Society

Newsletter for March 2014

Volume 32, number 2

563-265-1728

www.qcs.org

Computerized Investing SIG Returns in March

The Computerized Investing (CI) SIG has been rescheduled for the second Tuesday of the month at 6:00 p.m. starting on March 11th. Seven sessions are planned in 2014, with a summer break.

This year's first speaker will be Allen Holdsworth, the President of the Better Investing Volunteer Advisory Board. Better Investing is a national non-profit organization that teaches people how to be better investors. Allen has taught classes on investing in over 30 states and presented at the last seven Better Investing National Conferences. He was employed as a broker for seven years before retiring.

At the March CI SIG, his presentation will be "W**hen to Sell a Stock"** which is usually the hardest part of investing. Find out things to watch for to help make the decision that perhaps it is time to sell. Many indications that should trigger a sell will be discussed.

Allen will be back at the April 8th CI SIG to help us learn more about the Better Investing organization and how it provides information, education, and support for successful investing. He will tell us about the upcoming Better Investing National Convention that will be held in Chicago May 15-18th where he will be one of the presenters.

Check out: **www.qcs.org/investing.html** for the CI SIG 2014 schedule, planned presentations, and archived presentations from 2013.

Co-leaders, Darlene Norton and Vicki Wassenhove, look forward to seeing you at this informative SIG!

QCS: March Program How To Digitally Preserve Your Photos & Files

presented by
Lisa Huntsha
Archivist/Librarian at the
Swenson Center
Augustana College
lisahuntsha@augustana.edu

Lisa will present practical tips on how to preserve your family photographs and documents with a digital back up. She will discuss projects you can do in your home office using a scanner. She will also discuss preservation techniques and file management for your current digital content. Hardware, software, handling techniques, and work flow will be discussed.

Lisa Huntsha started her career in preservation while working at the Swenson Swedish Immigration Research Center during her time as a student at Augustana College. Inspired by her experience there, she went on to attend a master's program in Museum Studies at Syracuse University. She has since worked at historical societies, museums, and libraries in New York, Illinois, and Alaska. Now, she is back at her alma mater as the Archivist/Librarian at the Swenson Center where she does everything from processing archival collections to assisting researchers to hosting preservation workshops.

Views and opinions expressed by presenters do not necessarily reflect those of the Quad-Cities Computer Society. Monthly meetings are open to the general public.

We thank NBS, the host of the QCS.org site!

ENGAGE Network Business Systems Inc NBS

The QCS is a member of apcug An International Association of Technology & Computer User Groups

Would You Like to receive your *QBITS* via email?
The *QBITS* can now be produced in Acrobat PDF format and sent to your email box. If you desire to have the newsletter sent to you electronically instead of by US Mail, notify:
Patty Lowry,
QBITS co-editor
(563) 332-8679
pattylowry@rocketmail.com

QBITS
Published monthly by the
Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline, IL 61265
webpage: www.qcs.org
Co-editors
Joe Durham
joseph85_us@yahoo.com
Patty Lowry
pattylowry@rocketmail.com

The Quad-Cities Computer Society or QCS is an Iowa nonprofit organization for charitable, scientific, and educational purposes primarily to educate the public concerning the advantages and disadvantages of microcomputers and to publish a newsletter for distribution to members, area libraries and educational institutions. The QCS is recognized as a 501(c)(3) nonprofit charitable and educational organization by the IRS. Copyright *QBITS* copyright © 2014 by the QCS. All rights reserved. Subscriptions are included in cost of membership. Reproduction of any material herein is expressly prohibited unless prior written permissions is given by the QCS. Permission to reprint material contained herein is granted to other non-profit personal computer groups provided the full attribution of the author, publication title and date are given, except that articles with Copyright notice in the header indicates article may be reproduced with the express written permission of the author (or other indicated copyright holder). Brand or product names are trademarks of their respective carriers. As a typographic convention we do not so identify as such.

QCS Review: Practical Concepts for Protecting Your Computer: Its Data, Hardware and Data

by Larry Stone
Windows SIG leader
lstone521@mchsi.com

Larry has been guiding the Windows SIG for 19 years, and has worked with and repaired computers in that time frame as well. He has seen everything about computing: the good and the bad. It is with that foundation that he outlined for us practical solutions and safeguards to following when computing in this Internet age.

He began with a simple warning: **Do Not** download and install every program because it is free. Free software, can tag along malware, viruses, and ransomeware onto your computer for the price of the bargain. Always research any software before installing it. Download from only reputable sites like **Download.com.**

DO keep all of your program updates current. The software authors continually have to update their creations to keep malware from wrecking our computing experience. So update your Java, your Flash, and Windows.

As you make these updates you have to read all the fine print and make sure you *un-check* any unnecessary addons that these updates contain. For example, a Java update would like you to install a toolbar. Don't do it, leave that unchecked. The Adobe update would like to install Google Chrome as your default browser. Don't check that option before you install the Adobe update.

These methods are the current trends. So you must be an active participants in these selections or the updates will slow down your computer.

When browsing the Internet you need to take a proactive stand as well. On web pages you will often see videos, and ads on the right hand side of a web page. **Do Not** click on these things. It is an opportunity for these ads to insert malicious code into your computer. If you click on them, you are essentially saying yes go ahead and mess with my computer. Anti-virus and Malware seeking software cannot protect your from the conscious choices you make on the net. So be alert.

Larry noted that if you see something in these ads that interest you, go to their web site directly. Recently he saw an ad about Verizon, his cell phone company. He is about to get a new cellphone. So instead of clicking on the ad, he went directly to the Verizon website, where you can browse and read about the deals currently available direct from the manufacturer.

As you use the Internet you have to proactively monitor your email. **Do Not** open an email attachment, even if it is from someone you know, as it may contain malware or a virus. Make sure that you are expecting an attachment from your friend.

Recently, Larry has gotten an email from his granddaughter that contained a single link to an obscure web address. He deleted it. It is his theory that others on Facebook have made the link to his email using his granddaughter's Facebook postings. So as a word to the wise treat unknown attachments

with great caution.

Also it is a web courtesy do not forward emails. If you wish to share something, copy it to the clipboard and paste into a new email to your friend.

Despite our best intentioned efforts, there exist programmers who can't wait to make money out of your computer malady. The Crypto-Locker ransomeware that was featured in last months' QBITS is a prime example. In this case, Larry observed there is no defense once it is on your system. He and his friend Dale attempted to rescue a Crypto-Locked machine without success. They used every software tool at their command, and it just did not work. They had to reformat the drive, the person lost their data, and they had to start over.

So if you haven't been infected by this nasty Internet scheme, the old defense it to back up your data and software ahead of time, so that you can restore your machine to its original form with ease.

How do you do this? Larry recommended several easy steps. Your goal is to back up your data and software in its entirety and place it in several different locations so that the backup cannot be affected and infected by malicious programmers.

Purchase a good sized flash drive 32 GB or larger, and an external usb hard drive (standard versions are 500 GB), and subscribe to a free cloud storage account: Dropbox, Google Drive or OneDrive or Carbonite.

First make a Hard drive image of your entire computer and place it on an external usb hard drive. You accomplish this in Windows by going to the Control Panel → Backup and Restore → Create a System Image → To an external drive.

This process will work in the background while you use your computer. When finished, Larry recommends that you open up the Control Panel again → Backup and Restore → now Create a System Repair Disc.

Now you have done two things: you will have backed up your entire system, and secondly you will have created a disk that would allow you to recreate that entire image on a new hard drive if you current one fails.

Now that your entire system is backed up you can focus on backing up documents incrementally each day. For this function you don't need a great deal of space and your storage space choices are multiple: the flash drives of 32GB, Dropbox (**dropbox.com**) offers 5 GB of free space, OneDrive (**preview.onedrive.com/**) from Microsoft offers 7 GB of storage, Google Drive (**drive.google.com**) offers 15GB of storage. Carbonite (**Carbonite.com**) offers unlimited storage space online for a subscription fee of $59 / year.

Ccleaner **(www.piriform.com/ccleaner**) is a software tool that Larry recommends. It helps to delete temp files and the registry cleaner within keeps program associations tidy and functional. Run Ccleaner once a week.

Additionally your can improve the speed of your browser by periodically refreshing its settings. You accomplish this in Internet Explorer by going to Tools → Internet Options → Connection → Lan → making sure that the “Automatically detect settings” is checked. Also go to Tools → Internet Options → Advanced → click Restore Advance Settings. This will reset the browser to its original configuration.

In the second part of Larry's presentation he moved from software control to hardware investigation and repair. If you see your computer acting strangely, or your hard drive is making strange sounds. **Do Not** keep trying to boot up the computer when it locks up. By continuing to do so without addressing the core physical issues on the computer, you will eventually crash the hard drive. Recovery at this stage is very difficult, not free and expensive. Take you system to a technician for repair.

Larry noted that a Hospital did not have a back up system, and they badly needed the data on the failed drive. The only recourse was to send the hard drive to the manufacturer. They completely disassembled the drive and recovered the data at a cost of several thousands of dollars.

If you computer behaves strangely, **STOP**, take it somewhere so that an expert technician can attend to it before it fails completely.

Other hardware fail points that can occur from time to time are: bad memory chips, bad keyboards, leaking capacitors on the mother board (in which case a new motherboard is required). So when you encounter these events, a hardware repair is in order before your situation is unrecoverable.

Finally is it useful to secure your Internet connectivity to keep your system from the prying software fingers of hackers. You do this by turning on Microsoft's software firewall. If you have a high speed connection and use a router, you are in

--continued on next page--

a good position. The router will also act as a hardware based firewall and additional protection.

Additionally, **Do Not** use your Name as your wireless SSID. Larry uses a series of numbers for his wireless setup. You can also configure your wireless router to hide your SSID. This would be a good option if only you are using the wireless Internet service. Otherwise guests, and family would not see your SSID if you gave them permission to access your Internet connection.

Being a wise, secure and useful member of the Internet computer community requires active participation on your part. By following faithfully Larry's suggested tips and remedies, you will have a more smooth and less stressful computing experience, and get the most out of your machine.

The QCS would like to thank Larry for sharing is insight based upon many years of practical experience working with computers. His steps are real world tips to use.

Trewgrip

www.trewgrip.com

In the world of technology we witness many game changing inventions. The iPhone and smartphones are but two of many. When these new world devices appear, there also emerge branching technological inventions that attempt to improve or help us use these devices in a better or a unique way. The Trewgrip fits the branching category and helps to fill the gap of typing on a smartphone more easily than using our thumbs or fingers across the screen. The following image are a self-explanatory display of this solution.

1. Illuminated Visual Cues
When a key on the back is pressed, the corresponding indicator key on the front illuminates. This helps the user to easily locate the typing keys on the back using hand-eye coordination.

2. Universal Mobile Dock
Dock mobile devices (up to 5.3" wide) using a suction mount and Bluetooth connection to type more effectively on-the-go.

3. Thumb & Mouse Keys
Press the Tab, Enter, Space and Backspace keys using your thumbs on the front side (3.1). Use your right-thumb to click the left and right mouse buttons (3.2).

4. Navigation & Control Buttons
Additional front-side functions keys to make your text entry as efficient as possible. Use the navigation and control keys to move the cursor around within a block of text and to control the software.

1. Rubber Handgrips
Grip confidently and type comfortably with your choice of small, medium or large rubber handgrips in black, red, blue or TREWGrip green.

2. Ergonomically Curved Shape
The curved shape affords users the option to type while sitting, standing or walking. Easily reach the inner rows of typing keys without having to adjust your grip.

3. Lithium-ion Battery
Keep the lithium-ion battery charged with a mini-USB to USB cord. With an estimated battery life of up 10 hours, you'll have plenty of time to type on the go.

4. Mobile QWERTY Key Layout
Using the same key layout as a traditional keyboard (only split and rotated), users can transfer their typing knowledge from QWERTY to mobile QWERTY with only 8-10 hours of practice.

Smart Appliances, New Target for

Hackers, Already Compromised

by Ira Wilsker
iwilsker(at)sbcglobal.net

WEBSITES:
Proofpoint
goo.gl/VhFQT8

Refrigerator Hacked
goo.gl/spPF14

Refrigerators and Other Home Appliances
goo.gl/c8auYw

Phishing
goo.gl/SQcdgQ

Refrigerator Hacked
goo.gl/PdeFSp
Smart Refrigerators
goo.gl/lUlupf

Hacked Refrigerator Reveals Security Gaps
goo.gl/P2d05F

Can Smart Appliances Get Hacked and Turn on You?
goo.gl/zdGl4q

In recent years, I was a regular attendee of the massive, annual, Consumer Electronics Show (CES) held in Las Vegas. A few years ago, one category of items that most piqued my attention were the smart appliances. These smart appliances were early generations of major appliances that incorporated a functional computer in their design that offered the consumer a multitude of benefits. While many of the items demonstrated at the CES events that I attended were functional prototypes, some of the appliances are now making their way into the retail market.

Sometimes called "internet connected appliances", these smart appliances incorporate a small flat screen monitor, often a touch screen, that is somewhat similar to the common tablet computers that are readily available and often inexpensive today. Most of these internet connected appliances utilized the existing Wi-Fi connection, now common in many American homes, to communicate over the internet with the outside world. Almost all of these internet connected smart appliances used early versions of Google's Android or Microsoft's Windows operating systems. One company displayed major household appliances, such as a washer and dryer pair, that had a Wi-Fi connected touch screen not just to control the selection of functions, but also reported to the consumer such information as operating condition, malfunctions, service information, recalls, and other important facts about the appliances, utilizing the display along with emails and text messages to the consumer. Service calls could also be scheduled on the integral touch screen for any routine maintenance or repairs, with the device itself informing the technician of the problem and any required replacement parts before he leaves his shop for the consumer's home.

I was especially impressed with a prototype refrigerator that had a dedicated computer imbedded in it that was Wi-Fi connected, performed functions similar to the washer and dryer previously mentioned, plus added a UPC code reader to the functionality. The consumer could scan the UPC code of a grocery item with the device's reader, and create a printable shopping list. What was even more exciting was connecting the refrigerator via Wi-Fi and the internet to a simulated supermarket; the shopping list was printed in the order that the scanned items would be found in the supermarket aisles, or the order could be sent to the supermarket, with the desired groceries being carted by market employees for pickup or delivery. The simulated supermarket displayed its current ad on the device when requested, recommended sale items for selection or substitution, created digital coupons which could automatically be credited at time of purchase, and would otherwise save the consumer time and money.

These smart appliances are not some figment of science fiction, but are already appearing in peoples' homes. A quick visit to the store or website of any major seller of flat screen televisions will make abundantly clear the wide assortment of smart TV's currently for sale. These TVs are intended to connect to the home's broadband internet connection either via Ethernet (common networking cable), Wi-Fi, or direct internet connection provided by the cable or satellite providers. Web based services from the likes of Netflix, HuLu, Amazon Streaming Media, YouTube, and other digital content providers can already be received seamlessly on many of the TVs already in use and in the stores. These internet connected TVs currently available have substantial computer power built in to them, and run mostly on variations of existing operating systems from Apple, Google (Android), and Microsoft. as well as a few proprietary operating systems.

With the introduction of internet connected smart appliances, it was inevitable that someone would find

--continued on next page--

a way to hack into them for nefarious purposes, which indeed has happened recently. In the past few days the media has been rife with stories of hacked smart appliances, mostly refrigerators, that have been incorporated as "zombies" in a "botnet" or cluster of purloined or hijacked smart devices, and used to send out massive quantities of spam and phishing (attempted identity theft) emails.

In a published claim by the security company Proofpoint, (**goo.gl/VhFQT8**), released on January 16, 2014, " Proofpoint Uncovers Internet of Things (IoT) Cyberattack - More than 750,000 Phishing and SPAM emails Launched from "Thingbots" Including Televisions, Fridge". In their press release announcing the discovery of this form of cyber attack, Proofpoint stated that it " ... has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks. As the number of such connected devices is expected to grow to more than four times the number of connected computers in the next few years according to media reports, proof of an IoT-based attack has significant security implications for device owners and Enterprise targets."

Later in the same report, Proofpoint reported that cyber criminals have started to hijack soft targets in consumers' homes, including " ... home routers, smart appliances and other components of the Internet of Things" turning these intelligent devices into "thingbots" for the purposes of sending spam emails, committing identity theft, and a variety of other malicious activities. Proofpoint explains that these early generation smart appliances are "soft targets" because they were not designed and built with strong security measures in place, making them easily vulnerable to attack and hijack. These smart devices are especially attractive to miscreants for targeting because they do not typically incorporate the level of security widely utilized by more established technologies, including PCs, laptops, and tablets. These new smart devices are especially vulnerable to attack because they are poorly configured in terms of security, and often incorporate only factory default passwords; the default passwords have been widely circulated in hacker circles, and since similar devices often have the same default passwords, if one can be hacked into, they all can be hacked into. Also because these smart, internet connected devices have insecure default passwords, there is no need to use more traditional malware methods, such as trojans and viruses, to compromise those devices. At present, there is no readily available method or software that can secure these smart internet connected devices, such as there is security software and hardware available for PCs, tablets, and laptops.

The "thingbots" that Proofpoint uncovered was monitored by Proofpoint from December 23, 2013 to January 6, 2014. During this two-week period, waves of spam emails were often sent in bursts of 100,000, about three times a day. Of all of the spam emails monitored during this time, about one-fourth were sent by this "Internet of Things" consisting of the purloined multimedia centers, internet connected smart TVs, home routers, and at least one internet connected refrigerator. Each device connected to the internet has an IP (Internet Protocol) address that identifies it to the internet; in this deluge of spam and other malicious emails, no more than 10 emails were sent at any one time from any individual device, making them difficult to block by traditional anti-spam blocking methods. Since such a small number of emails were sent at any one time from any compromised smart device, users would not likely have noticed any decline in device performance. If these same devices were to be used (as they still may be used in the future) for launching any massive, crippling "DDoS attacks" (Distributed Denial of Service attacks) used to shut down targeted internet servers and websites, then the users may notice a distinct decrease in performance of their devices, as their internet connectivity may be heavily used for nefarious purposes.

According to Proofpoint, this "Internet of Things", or IoT is massive, and increasing at a very rapid rate, compounding the massive degree of cyber threats that these devices may pose when compromised. In its posting on the problem, Proofpoint stated, "IoT (Internet of Things) includes every device that is connected to the internet - from home automation products including smart thermostats, security cameras, refrigerators, microwaves, home entertainment devices like TVs,

gaming consoles to smart retail shelves that know when they need replenishing and industrial machinery – and the number of IoT devices is growing enormously. IDC predicts that more than 200 billion things will be connected via the Internet by 2020."

While these internet connected smart devices hold great promise to consumers and businesses, and become even more widely used than they are today, both the manufacturers of these devices and third party security vendors must devise a way to secure them from attack and hijacking. Just imagine if your internet connected home security system is hijacked allowing burglars unfettered access to your house; your smart home thermostat is hijacked by cyber vandals while you are away from home, and either make the home very cold or hot, especially during a freeze o heat wave; hijacked smart refrigerators run at improper temperatures, causing damage or destruction to the contents inside; microwave ovens cook for unintended times and power; and other potential unintended consequences of having insecure technology in our homes and businesses.

In order not to kill their extensive and growing market, it is inevitable that the makers of these "Internet of Things" devices will soon devise a way to secure these useful products.

gary.stanley.net/cyber_news.htm

Well, 2013 is history and it's time to start thinking about collecting receipts and getting things in order for your income tax return. Of course it's a tendency for most of us to put this off till the last minute. You have to wonder what Warren Buffett's return looks like. I find it incomprehensible that Mr. Buffett made 37 million dollars a day last year. Yes, I said a day! The legendary billionaire and philanthropist finished 2013 with a net worth of $59.1 billion, up from $46.4 billion at the beginning of the year. Yes, the rich get richer! Get the low down from Market Watch. **goo.gl/eDgSW0**

Of course money doesn't create happiness. Most of us would love to win the lottery, but would we really? It's a fact that most lotto winners lost it all and are very unhappy people. Winning the lottery would create so much stress into our lives that it would be almost unbearable especially in those states that require your name to be released. Let me put in this paragraph what always appears at the bottom of the page in every Cyber News, and that's my motto. "Live with Passion, in a constant state of Joy, and with an Attitude of Gratitude"! Be grateful for what you have and your life will be happier!

Take a stroll down memory lane and look at events that influenced 2013. What was your biggest memory of last year? Was it the papal transition, the Zimmerman trial, the Royal baby birth, the Boston bombing, or maybe the Jodi Arias trial? Some of these events were negative, but perhaps you had a wonderful personal memory of the year. Yahoo has provided a site that will showcase highlights, and you could probably spend all day clicking on different stories! Take a look. **goo.gl/7LJa3z**

Curtain calls 2013: Remembering stars, old and young, who passed last year. Actress Bonnie Franklin, Annette Funicellow and comedian Jonathan Winters are just three. The story from NBC's Today. **goo.gl/wQNecT**

Super Bowl 2014. Get ready everybody; this is going to be a Super Bowl of firsts. **goo.gl/OFVLbV** Aside from being the first outdoor, cold weather Super Bowl, Super Bowl XLVIII is also the first to be hosted by two states. February 2nd is the big game and commercials on the Fox network have been sold out for some time. The rate? How about 4 million dollars for 30 seconds! Who bought the spots? Here's the scoop! **goo.gl/vSCvRO**

This year amateur film makers were invited to make 30 second Super Bowl commercials for Doritos. From what I understand one of the finalists will be played during the game. I watched five of them and they are really good! Take a look. **goo.gl/SblKtM**

Will Amazon and other companies be sending you Christmas presents via a drone next year? It's hard to imagine drones delivering packages. What kind of a mess will that make for our skies? But this is definitely in the planning stages. The story from Forbes. **goo.gl/wgeqDr**

For years our computers came with a program called "Media Player." It would play all your music and videos, but what a lot of people didn't realize is it would also take you to the Internet for other options. You could listen to radio stations, preview movies, play games, and all kinds of fun stuff. With Windows 8 however, as with everything else, things changed and the button that took you to the Internet is no longer there. Kind of like the disappearing Start Button.

--continued on next page--

After installing new computers for customers and being embarrassed as to where they were hiding this feature, I researched and found that now the fun is on a website. Check it out **goo.gl/vdMzYc** and bookmark it so you can go there often.

I should have put this site in Cyber News last month because it's a great place to find gadgets for your cell phone, along with other neat things. Would have been a good place to visit for Christmas gifts, but it's never too late for 2014. You'll have a blast checking out all the goodies! **goo.gl/AJY1jk**

Get a new computer or laptop for Christmas? If so, and if it's a PC, your operating system is Windows 8 and the best thing you can do to make your life not so frustrating is to install "Classic Shell." That's a third party Start button that will make you more at home with the new system and you can find it here. **goo.gl/t0MGOn**

Get a new iPad for Christmas? If you did, you must get the app "Flipboard." I sit on the couch every night, while watching TV, and flip through all my favorite news sources. It's the greatest app on my iPad and it's free! Also, here are some great tips **goo.gl/oCXgNW** if you have an iPhone or an iPad!

Meet "Wisp," the wireless future of the Internet. The Internet connection we all rely on is about to change, now that WISP is coming to town. No more cable or telephone connections to get to the Internet. As if technology wasn't good enough today, tomorrow it's getting better! Read all about it from PC World. **goo.gl/LnFQeJ**

You undoubtedly heard about the theft of 40 million credit accounts from shopping at Target. If you shopped there between November 27th and December 15th and used your credit card, you are at risk. The worst part of this scenario is that cards are being sold on the black market. Here's my take. If I were one of those persons I would cancel my card and have a new one issued. That is the only safe thing to do. Many stories have appeared on the Internet and here is one of them from CNET. **goo.gl/OBHXOK** Credit card hacks will continue happening because our credit card system in America is antiquated. That story from CNN. **goo.gl/2kyMxM**

Ever notice a spot on your body? If it looks a little out of the ordinary and doesn't want to go away, don't ignore this as it may be skin cancer. The first step is to find a good dermatologist and have it checked. If suspicious he or she may want to do a biopsy. Don't worry, this is not a big deal, cause I've recently gone through this. My spot was just below my left eye and was diagnosed as basal cell carcinoma and I went through a simple surgery to remove it. Read about it in my Blog. **goo.gl/6GrUj7**

I can remember television sets when they had black and white pictures and snowy at that! The TVs of today feature pictures that make you think you're in the scene. I recently saw an 80 inch model in a store that took my breath away. Now LG and Samsung have announced a 105 inch ultra HD TV. Wow! Details from NBC. **goo.gl/J57yPF**

A lot of Internet sites require you to log-in with a user name and password. This is especially important when using banking sites, but the question is do you log-off when finished? Not doing so leaves your account open and that's not good. Here's a further explanation. **goo.gl/f9QSBk** Remember also never to use the same password for all accounts. If a hacker guesses one, he has them all!

Imagine the year 2020: Augmented reality glasses like Google Glass are everywhere. Cars are connected and, in some cases, driverless. Your smart phone is less a phone than a command center uniting the various nodes of your technological self — watch, glasses, wallet and car alike. But what about your personal camera? What will it look like in 2020? The story from USA Today. **goo.gl/2xarvs**

The year 2020 is a few years away, but 2014 is here now and so let's imagine what it will be like. Albert Einstein was quoted as saying "Imagination is everything. It is the preview of life's coming attractions." So let's imagine a Happy 2014!

NOW I KNOW
THAT'S HALF THE BATTLE!

nowiknow.com

Wi-Fido

We're still probably a few years away from universal wi-fi in the developed world. Many municipal wireless networks are planned or in the works, but there are few currently existing. **goo.gl/z6i73M** As we progress toward access-everywhere, both public institutions and private telecom companies (often working together) are finding creative ways to provide service in places we'd otherwise refer to as "dead zones." In New York City, for example, some subway platforms now have free wi-fi service, **goo.gl/IIY2YB** but users need to watch (or more likely, ignore) a 15

second video before access the rest of the universe's content.

But no one has been as creative a company in Mexico which decided to provide somewhat-free wi-fi in a handful of public parks. "Somewhat-free" because while it won't cost users any *money*, they need to deposit *something* to get online. That something?

Dog poop.

Terra is a Spanish-language Internet portal (like Yahoo!) which has a large audience in Mexico. As part of a marketing campaign dreamed up by their agency, DDB Mexico, the company placed wi-fi hotspots in ten parks in the spring of 2012. To access the invisible beams, though, would-be customers had to pick up after their dogs and dump the waste in a big bin. The bin weighed the dog doo and rewarded everyone in the park with some free wireless minutes. The more poop scooped, the more minutes granted.

And, this being the Internet age, DDB and Terra made a promo video, available below, about their endeavor.

goo.gl/ntrnaz

Of course, the system could be gamed. As CNET pointed out, **goo.gl/O0qhwI** the machines have "a simple scale to weigh the poop, so they would likely still work if people put rocks or trash in them instead." Terra seemed OK with this — loophole-lovers who picked up litter would help keep the parks clean, too — but in any event, there may have been some informal policing. As Creativity-Online reported, **goo.gl/xsNwLp** the wi-fi hotspots weren't left unattended: "to help consumers focus on the poop, however, hostesses manned each of the bins during the day, passing out bags for doggie droppings."

Bonus Fact: What does "Wi-Fi" stand for? According to Boing Boing, absolutely nothing. **goo.gl/6GVps3**

Nominating Committee Report for 2014

At the opening of the program meeting March 3rd, a report of the nominating committee will be presented. After presenting this slate, the President will open the meeting for nominations from the floor. Floor nominations require that:

1) Nominees must be members in good standing.

2) Nominees must be present and express their willing ness to serve.

3) Any nominee not present must have submitted to the Board prior to the meeting by mail to Diana Wolf, Secretary, Quad Cities Computer Society,, 46 Wilwood, Moline, Il 61265 a written statement expressing their willingness to serve if elected.

President:
Judi McDowell
Vice-President:
Ralph Drexler
Secretary:
Darlene Norton
Treasurer:
Dave Tanner
Corresponding Secretary:
Shari Peterson

Directors at Large:
Janice Aquirre
Jim Buche
Jack Boocarosa
Joe Durham
Marie Drexler
Patty Lowry
Melinda Missman
Sue Peterson
Karen Reynolds
Emily Smith
Diana Wolf

Submitted by Joe Durham Nominating Committee Chair

Gmail : Who Is Using It? BobG-vast!

Bob Gostischa, has posted a very informative tip about protecting your Gmail account. Go to this YouTube video tutorial : **youtu.be/JxEsj0MAS1E**

Also to view your ip address, in your browser type:

whatismyip.com

Interesting Internet Finds

Steve Costello, Boca Raton Computer Society
(reprinted from the February 2014 issue of *Boca Bits*)
editor@brcs.org
ctublog.sefcug.com/

In the course of going through the more than 200 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 January 2014.

Hashtags Today Are Everywhere – Learn How To Use Them To Get Results
goo.gl/ofdsu6

--continued on next page--

Hashtags are not only for Twitter, this post shows other social media that use them, and how to use them effectively there.

How to Move Apps to SD Card on Your Android Device
goo.gl/kJSguX

This question was asked at a SIG (Special Interest Group) earlier, but no one had an Android device with an SD card, so could not answer the question. This post refers to an app to do that.

Google Plus Login, Sign Up and Sign In Security Tips
goo.gl/qJcErh

Thinking of signing up for Google Plus? If so, and I think you really should check it out, read this post from the Windows Club for how to do it.

You can find me on Google Plus at: **goo.gl/w2zeMA**

How to Read a Kindle Book on a Computer
goo.gl/5u2dtY

This post explains how to read Kindle books without a Kindle device, or smartphone, by reading it on your computer via two different methods.

Remove Personal Information from Your Digital Photos
goo.gl/Nwxf0S

Concerned about personal information showing on your online photos? If so, check out this post for how to remove the information before posting with Windows Explorer.

If External Hard Drives Can Fail, Should I Bother With One?
goo.gl/dMRphO

Leo answers with a definitive YES, and explains why.

Officers 2013-2014

Elected Officers

President	Judi McDowell	(309) 314-1780	julee89@gmail.com
Vice President	Ralph Drexler	(309) 755-8138	drexlerrm@mchsi.com
Secretary	Maggie Gillespie	(563) 332-5661	m.gillespie@mchsi.com
Corresponding Secretary	Shari Peterson	(563) 468-1658	skp4joy@gmail.com
Treasurer	Dave Tanner	(309) 764-6455	dl.tanner@mcshi.com
Directors at Large	Jim Buche	(309) 755-4893	jhbuche@mchsi.com
	Marie Drexler	(309) 755-8138	drexlerrm@mchsi.com
	Tina Gean	(309) 373-1122	tina2121@yahoo.com
	Melinda Missman	(309) 235-7579	mamissman@gmail.com
	Susan Peterson	(309) 721-7048	felspaw@gmail.com
	Emily Smith	(309) 794-9320	ginghis18@mchsi.com
	Diana Wolf	(309) 797-5413	
Director Past President	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com

Director/SIG Leader

Beginners	Jim Kristan	(309) 755-8277	jmkris@gmail.com
Genealogy	Len Stevens	(563) 359-9672	judylenstevens@msn.com
Digital (coordinator)	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
Internet	Ted Huberts	(309) 792-9470	slowhand54@sbcglobal.net
Office	Judi McDowell	(309) 314-1780	julee89@gmail.com
QBits	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Windows	Larry Stone	(309) 787-5574	lstone521@mchsi.com

Appointed Officers

Membership Director	Susan Peterson	(309) 721-7048	felspaw@gmail.com
Program Director	Ralph Drexler	(309) 755-8138	drexlerrm@mchsi.com
Public Relations Dir.	Melinda Missman	(309) 235-7579	mamissman@gmail.com
Publicity	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Financial Committee	Mel VanderHoek	(563) 505-9661	vanderhoek@netexpress.net
APCUG Representative	Patty Lowry	(563) 332-8679	plowryapcug@gmail.com
Membership Records	Susan Peterson	(309) 721-7048	felspaw@gmail.com
Web Master	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
QBITS Newsletter	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Mailing	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Resource Manager	Judi McDowell	(309) 314-1780	julee89@gmail.com

MEMBERSHIP CORNER

Membership dues are payable **July 1st** each year and expire the following **June 30th**.

Individuals	$30
Family	$40

Payments can be made in person at a meeting or mailed to the treasurer

David Tanner
3449 – 52nd Street
Moline, IL 61265

SIG and Event Calendar

March ২০১৮

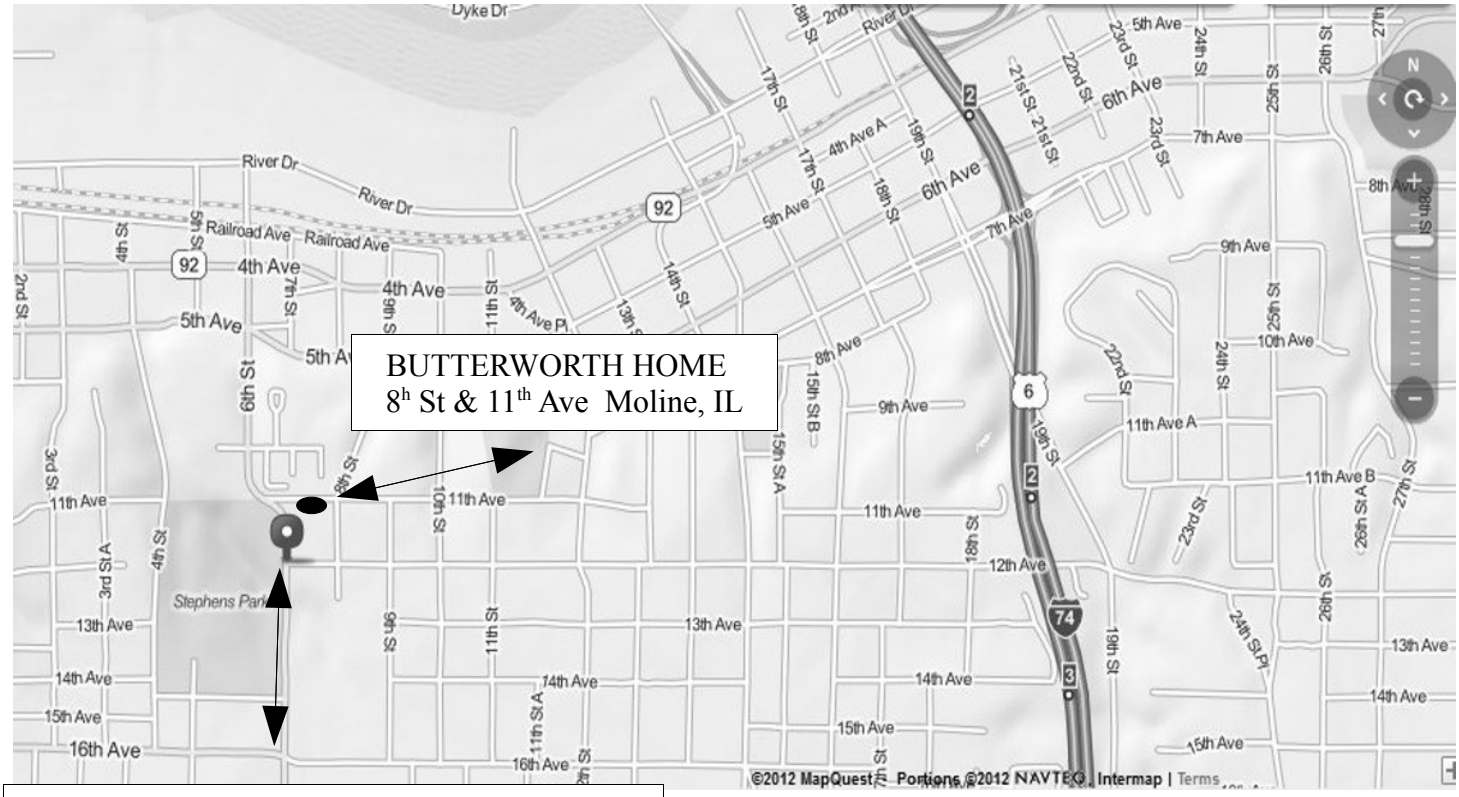
Mar ৩th – Mon	৭:৩০ PM	**Beginners SIG**	EDC	Jim Kristan	৩০৫-৩৭৭-৫২৩৩
	৩:০০ PM	**How to Digitally Preserve Your Photos & Files**	EDC		
Mar ১৩th – Mon	৭:৩০ PM	Genealogy SIG	EDC	Len Stevens	৭৫৩-৩৭৫-৫৫৩২
	৩:০০ PM	Internet SIG	EDC	Ted Huberts	৩০৫-৩৫২-৫৮৩০
Mar ২৮th – Mon		Digital Media SIG	EDC	Vicki Wassenhove	৩০৫-৩৫৩-২২৩৫
	৩:০০ PM	Windows SIG	EDC	Larry Stone	৩০৫-৩৫৩-৭৭৩৮

Location Key

BCL Library of Butterworth Home
CRA Craft Room of Butterworth Home
EDC Education Center of Butterworth

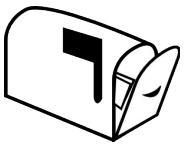
Location Key

MVC Moline Vikings Club
OAK Oak Room of Butterworth Home
ORC Orchid Room of Butterworth Home



EDUCATION CENTER OF BUTTERWORTH
7th St & 12th Ave Moline, IL

Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline IL 61265



Moving? Send an address change to:
felspaw@sbcglobal.net

This Month in *QBITS* ....

Monday
March 3th
7:00 PM

How To Digitally Preserve Your Photos and Files

presented by
Lisa Huntsha
Archivist/Librarian at the Swenson Center
Augustana College